FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

DECISION NOTICE

To: **Standard Chartered Bank**

Firm Reference Number: **114276**

Address: **1 Basinghall Avenue**
London
EC2V 5DD

Date: **5 February 2019**

1. ACTION

1.1. For the reasons given in this Notice the Authority has decided to impose on Standard Chartered Bank ("SCB") a civil penalty of £102,163,200.

1.2. SCB agreed to settle in relation to all relevant facts and all issues as to whether those facts constitute breaches. SCB therefore qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £145,947,500 on SCB.

2. SUMMARY OF REASONS

2.1. On the basis of the facts and matters described below, SCB breached Regulations 14(3), 15(1) and 20(1), and failed to comply with Regulations 7(1) to (3), 8(1) and (3), and 14(4) of the Money Laundering Regulations 2007 (the "ML Regulations") by failing to establish and maintain risk-sensitive policies and procedures, and failing to require its non-EEA branches and subsidiaries to apply UK-equivalent anti-money laundering and counter terrorist financing ("AML") standards regarding customer Due Diligence and ongoing monitoring.

Exhibit 13

2.2. The breaches concerned SCB's financial crime controls in two areas of its business which SCB identified as higher risk:

a. SCB's UAE branches in the period from 24 November 2009 to 31 December 2014 inclusive (the "Relevant Period"); and

b. SCB's correspondent banking business within its UK wholesale banking business in the period from 11 November 2010 to 22 July 2013 inclusive (the "CB Relevant Period").

2.3. The Authority found serious, and sustained, shortcomings in SCB's financial crime controls in the customer Due Diligence and ongoing monitoring carried out by SCB. For example, in one instance, SCB opened an account in the UAE for a consulate, funded with the equivalent of just over £500,000 brought into the UAE by the consul in cash, in a suitcase. SCB failed to adequately establish the source of funds and therefore to mitigate the increased risk posed by this transaction and this customer.

2.4. The Authority also found significant shortcomings in:

a. SCB's own internal checks on its AML controls;

b. SCB's approach towards identifying and mitigating material money laundering risks; and

c. SCB's escalation of money laundering risks.

2.5. Given that SCB's AML controls in the UK set global standards across the group as a whole, inadequate standards in the UK risked affecting the entire group. Frequently financial crime compliance is perceived within firms to be the responsibility of compliance or a few key individuals. SCB's experience demonstrates the need for everyone across the business to ensure financial crime controls are effective in mitigating financial crime risk.

2.6. Money laundering can undermine the integrity and stability of our financial markets and institutions. The UK is a global financial centre and UK banks, and their subsidiaries, operate around the world. The Authority recognises the difficult challenge of achieving consistent adherence to global policies. However, when banks fail to adhere to, and implement, their legal and regulatory obligations, it makes it significantly easier for criminals to launder money. It enables them to transfer and recoup the proceeds of their crimes and hurts the UK economy, and furthermore undermines the global AML system.

2.7. SCB's failings are particularly serious because they occurred against a background of heightened awareness within SCB of issues with its global financial crime controls arising from action taken by US regulators and prosecutors, direct feedback from the Authority, and through its own internal assessments. In addition, throughout the Relevant Period, the Authority, along with the UK government as well as international and domestic governmental organisations, repeatedly issued communications regarding jurisdictions with a high risk of money laundering and/or financial crime.

2.8. Despite these warnings, the Authority identified poor Due Diligence and ongoing monitoring in the customer files it reviewed; it observed a number of UAE customers where transactions were inconsistent with the business profile of the customer and customers for whom source of funds was unclear. The Authority further identified customers with links to countries subject to sanctions. The inadequate Due Diligence and ongoing monitoring not only exposed SCB to

sanctions evasion but also increased the risk of SCB receiving and/or laundering the proceeds of crime.

2.9. In light of the above failings, the Authority has decided to impose a financial penalty on SCB of £102,163,200 after 30% (stage 1) discount (£145,947,500 before discount) pursuant to Regulation 42 of the ML Regulations. Approximately 85% of this penalty, £86,322,300 after 30% (stage 1) discount (£123,317,600 before discount) relates to failings in SCB's oversight of its UAE branches, and £15,840,900 after 30% (stage 1) discount (£22,629,800 before discount) (approximately 15%) of this penalty relates to SCB's correspondent banking failings.

2.10. SCB is working with the Authority, as well as other regulators in various jurisdictions in which it operates, to improve its financial crime controls. SCB's current senior management has over the past 4 years instituted a range of measures across its business (set out in paragraph 4.123 below), including measures designed to improve its governance structure and oversight of its non-EEA branches and subsidiaries to ensure that the issues identified in this Notice are fully addressed.

3. DEFINITIONS

3.1. The definitions below are used in this Notice.

"AML" means anti-money laundering and CTF;

the "Authority" means the body corporate previously known as the Financial Services Authority and renamed on 1 April 2013 as the Financial Conduct Authority;

"beneficial owner" means the term as defined in Regulation 6 of the ML Regulations;

"CB Relevant Period" means the period from 11 November 2010 to 22 July 2013 inclusive;

"Consumer Bank" means the consumer banking division of SCB, which ceased to exist on 1 April 2014 (when SCB was reorganised into retail banking, private banking, commercial banking and corporate and institutional banking), together with those customer segments and product types in the post-1 April 2014 structure which originally fell within the Consumer Bank;

"Correspondent" – see definition of Correspondent Banking;

"Correspondent Banking" means the term as used in Regulation 14 of the ML Regulations and which is described in JMLSG Guidance, Part II, paragraph 16.1, as being the provision of banking-related services by one bank (the "Correspondent") to an overseas bank (the "Respondent") to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network;

"CTF" means counter terrorist financing;

"customer due diligence" and "CDD" mean customer due diligence measures as defined by Regulation 5 of the ML Regulations;

"DEPP" means the Authority's Decision Procedures and Penalties Manual;

"Due Diligence" means together customer due diligence and enhanced due diligence obligations;

"enhanced due diligence" and "EDD" mean enhanced customer due diligence measures. The circumstances where enhanced due diligence should be applied are set out in Regulation 14 of the ML Regulations;

"Extended Selection" means a selection of an additional 12 UAE customer files from the Consumer Bank all of which were subject to enhanced due diligence at account opening, and all of which were closed during the Relevant Period;

"FATF" means the Financial Action Task Force which is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The FATF recommendations provide international standards on combating money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction;

"Financial Crime Risk" means SCB's Financial Crime Risk function (subsequently renamed Financial Crime Compliance);

"GIC" means Group Introduction Certificate. SCB made use of GICs when introducing a customer of one SCB office (the sending office) to another overseas office (the receiving office);

"Handbook" means the Authority's Handbook of rules and guidance;

"iBanking" means SCB's online banking system that was predominantly used by SCB's retail customers;

"Iran Addendum" means a list of eight questions appended to SCB's Due Diligence policies applicable to the Consumer Bank in its UAE branches, developed in order to strengthen SCB's controls relating to the dealings of SCB's branches in the UAE with Iranian national customers purporting to be resident in the UAE. The questions were focused on obtaining evidence to establish the customer's UAE residency;

"JMLSG" means the Joint Money Laundering Steering Group. The JMLSG is a body comprised of the leading UK trade associations in the financial services sector;

"JMLSG Guidance" means the guidance that was applicable during the Relevant Period issued by the JMLSG, and approved by the Treasury, on compliance with the legal requirements in the ML Regulations, the regulatory requirements in the Handbook and evolving practice within the financial services industry. The JMLSG Guidance sets out good practice for the UK financial services sector on the prevention of money laundering and combatting of terrorist financing;

"KCSA" means Key Control Self-Assessment;

"ML Regulations" means the Money Laundering Regulations 2007, which were in force in respect of conduct from 15 December 2007 to 25 June 2017 inclusive;

"PEP" means Politically Exposed Person as defined in Regulation 14(5) of the ML Regulations;

"Rejected Transaction" means a transaction involving a customer of SCB's UAE branches which was rejected by a counterparty bank or another SCB branch/office as a result of concerns over the sanctions risks connected with the transaction;

"Relevant Period" means the period from 24 November 2009 to 31 December 2014 inclusive. See also the definition of "CB Relevant Period";

"Respondent" – see definition of Correspondent Banking;

"SAMLP" means Systematic Anti-Money Laundering Programme, which is a programme of 'deep dive' AML assessments conducted by the Authority;

"SAR" means suspicious activity report;

"SCB" means Standard Chartered Bank, which is a UK bank headquartered in London. SCB is the main regulated entity within the Standard Chartered Group;

"SCB GORC" means SCB's Group Operational Risk Committee;

"Standard Chartered Group" means the group of companies consisting of Standard Chartered PLC and its subsidiaries. Standard Chartered PLC ordinary shares are listed on the London Stock Exchange and Hong Kong Stock Exchange, and Indian Depository Receipts (IDRs) are listed on the Bombay Stock Exchange and National Stock Exchange of India;

"S2B" means SCB's online banking system (Straight2Bank) that was predominantly used by SCB's corporate customers;

the "Treasury" means Her Majesty's Treasury;

the "Tribunal" means the Upper Tribunal (Tax and Chancery Chamber);

"UAE branches" means SCB's licensed branches in the UAE. SCB's UAE presence consisted of 14 branches in three emirates across the UAE during the Relevant Period. SCB is also licensed to operate in the Dubai International Financial Centre, but this Notice makes no findings in relation to that branch;

"UAE CORC" means SCB's UAE Country Operational Risk Committee;

"UAE File Review" means the Authority's review of 98 UAE customer files and the Extended Selection;

"UK Wholesale Bank" means SCB's UK wholesale banking business;

"unwrapping" means identifying the beneficial owners and verifying on a risk sensitive basis the ownership structure of corporate entities;

"Wholesale Bank" means the wholesale banking division of SCB, which ceased to exist on 1 April 2014 (when SCB was reorganised into retail banking, private banking, commercial banking and corporate and institutional banking), together with those customer segments and product types in the post-1 April 2014 structure which originally fell within the Wholesale Bank; and

"Wholesale Bank CDD Policies and Procedures" means the AML policies and procedures that were in place within the Wholesale Bank during the Relevant Period.

4. FACTS AND MATTERS

Background

4.1. SCB is a global bank, headquartered in London which provides a range of financial products and services for personal and business customers. SCB comprises a network of more than 1,109 branches and outlets in 68 markets.

4.2. UK firms are required by the ML Regulations to establish and maintain appropriate and risk sensitive policies and procedures in order to minimise the risk of their being used by those seeking to launder the proceeds of crime, evade financial sanctions, or finance terrorism. This includes conducting Due Diligence and ongoing monitoring. UK firms also have a duty under the ML Regulations to require their non-EEA branches and subsidiaries to apply AML standards at least equivalent to those required in the UK in relation to Due Diligence and ongoing monitoring.

4.3. These financial crime controls are particularly important for SCB as:

a. it operates extensively in major financial hubs which, from the scale, volume and values of the business conducted, and/or the geographical location of those hubs, might present a higher risk of financial crime;

b. its broad offering of products and services includes those which could present a higher risk of financial crime, such as Correspondent Banking; and

c. it operates on a global basis. In certain circumstances, once a customer had been accepted in one jurisdiction, the same customer can be offered products and services by SCB branches and subsidiaries in other jurisdictions. As such, any AML control inadequacies in one jurisdiction can, and in fact did, impact other jurisdictions.

4.4. SCB's UK head office is key to SCB's AML control framework because:

a. SCB's UK AML controls form the basis for the controls to be applied in its non-EEA branches and subsidiaries; and

b. it is responsible for ensuring the adequacy of AML controls in its non-EEA branches and subsidiaries.

4.5. SCB has licensed branches in the UAE serving over 340,000 customers throughout the UAE, the Middle East, North Africa and beyond. Its UAE presence consists of 14 branches, with its main office in Dubai. The UAE is SCB's seventh highest earning region across its Group. SCB considered its UAE branches to be a high financial crime risk environment, in part because of the UAE branches' geographic proximity to sanctioned countries, including Iran. Customers of SCB's Wholesale Bank included larger corporate entities than customers of the Consumer Bank. The financial crime risks associated with Wholesale Bank customers, products, delivery channels and geographical areas of operation can be different from those of the Consumer Bank.

4.6. During the CB Relevant Period, the UK Wholesale Bank had Correspondent Banking relationships with 1,314 financial institutions in non-EEA jurisdictions. The UK Wholesale Bank undertook almost 1.9m transactions with those customers at a total value of approximately $1.14trn during the period from November 2010 to July 2013 inclusive. Among other things, the UK Wholesale Bank provided cash and clearing services to those customers. The UK Wholesale Bank undertook the second highest value of Correspondent Banking cash transactions within the Standard Chartered Group in 2012 and 2013.

4.7. SCB was profitable throughout the Relevant Period; its pre-tax profits ranged between a high of $6.7bn generated in 2012, to $4.1bn generated in 2014. SCB's 2014 Annual Report indicated that approximately 90% of the income and profits generated by SCB and its subsidiaries was earned from its operations in Asia, Africa and the Middle East.

4.8. SCB's official accounting currency is US dollars, as most of its business is carried out in US dollars, or currencies linked to the US dollar. Most figures quoted in this Notice are therefore in US dollars – this does not mean, however, that all transactions referred to in this Notice were carried out in US dollars.

Overview of AML legal and regulatory obligations

4.9. The ML Regulations provide that, when considering whether a failure to comply with the ML Regulations has occurred, the Authority will have regard to whether a firm has followed guidance approved by the Treasury, such as the JMLSG Guidance, or issued by the Authority.

4.10. Relevant extracts from the ML Regulations and JMLSG Guidance are set out in Annex A to this Notice.

Due Diligence and ongoing monitoring requirements

4.11. Customer due diligence, enhanced due diligence and ongoing monitoring are measures designed to reduce the risk that a firm will be used by those seeking to launder the proceeds of crime, finance terrorism or evade financial sanctions.

4.12. A firm must carry out CDD on its customers. This means:

a. identifying the customer and verifying the customer's identity on the basis of documents or other data obtained from a reliable and independent source;

b. identifying the beneficial owner(s) of the customer, and taking adequate measures on a risk-sensitive basis to verify that beneficial owner's identity; and

c. obtaining information on the purpose and intended nature of the customer's relationship with the firm.

4.13. If a firm has assessed that the business relationship with the customer presents, by its nature, a higher risk of money laundering or terrorist financing, it must conduct EDD. If a firm is not able to apply CDD measures, it must not accept the customer or perform any transactions with or for that person. If a firm is not able to apply CDD measures to an existing customer, the firm must terminate its existing relationship with that customer.

4.14. A firm must also conduct ongoing monitoring of all business relationships, tailored in accordance with the firm's risk assessment of that customer. Ongoing monitoring includes:

a. keeping CDD up to date through periodic review of the CDD file, or reviews of the Due Diligence in response to trigger events; and

b. scrutinising customer transactions to ensure that they are consistent with the firm's knowledge of the customer (including where necessary, the source of funds), its business, and risk profile.

4.15. Where the business relationship is considered to be higher risk, the ongoing monitoring must be enhanced, meaning more frequent or intensive monitoring.

4.16. Firms have an obligation to require their non-EEA branches and subsidiaries to apply CDD measures and ongoing monitoring measures at least equivalent to those set out in the ML Regulations.

Correspondent Banking requirements

4.17. Correspondent Banking is the provision of banking-related services by one bank (the Correspondent) to an overseas bank (the Respondent) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide itself, typically because of a lack of an international network.

4.18. As the Correspondent often has no direct relationship with the underlying parties to a transaction, it is reliant, among other things, on the AML controls of the Respondent to prevent the underlying parties from gaining access to the UK financial system for the purposes of money laundering or terrorist financing. The ML Regulations and JMLSG Guidance acknowledge that Correspondent Banking relationships with Respondents from non-EEA states present a particularly high risk of money laundering.

4.19. The ML Regulations therefore require Correspondents to carry out EDD and enhanced ongoing monitoring on non-EEA Respondents. In particular, the Correspondent must:

a. gather sufficient information about the Respondent to understand fully the nature of its business;

b. determine the Respondent's reputation and the quality of its supervision from publicly available information;

c. assess the Respondent's AML controls;

d. obtain senior management approval before establishing a new Correspondent Banking relationship;

e. document the respective responsibilities of the Respondent and Correspondent; and

f. satisfy itself that the Respondent has identified and verified the identity of its underlying customers who have direct access to the Correspondent's accounts, conducts ongoing monitoring of those underlying customers and is able to provide the Correspondent with relevant documents and information about them.

4.20. The ML Regulations stipulate that these requirements must be applied on a risk-sensitive basis.

Deficiencies in SCB's AML controls

4.21. The Authority found deficiencies in SCB's AML controls regarding its UAE branches throughout the Relevant Period, and its Correspondent Banking business within the UK Wholesale Bank throughout the CB Relevant Period.

4.22. SCB's AML control deficiencies included failings in:

a. Due Diligence – see paragraphs 4.23 to 4.61; and

b. ongoing monitoring – see paragraphs 4.62 to 4.80.

Deficiencies in Due Diligence: SCB's UAE branches

4.23. SCB failed to ensure the AML controls which it required its UAE branches to apply were at least equivalent to those required of a UK firm. Throughout the Relevant Period SCB failed to ensure that its UAE branches:

a. collected sufficient information on the customer and analysed that information in order to understand the nature and purpose of the customer's accounts and businesses; and

b. consistently established the source of funds of the customer to enable an assessment of whether the risk(s) associated with the customer was likely to materialise.

4.24. Without this information, SCB's UAE branches were unable to identify and assess adequately the risk associated with a business relationship. This impeded SCB's ability to manage its money laundering and terrorist financing risks effectively, and establish a basis for monitoring customer activity and transactions.

4.25. The Authority assessed the quality and effectiveness of Due Diligence (and ongoing monitoring) in a review of customer files in SCB's UAE branches in November 2014. The review predominantly examined small and medium enterprise customer files, but also other categories of customers which SCB considered to be high risk, or where enhanced EDD was required.

4.26. The Authority later reviewed an additional 12 customer files from SCB's UAE branches (the Extended Selection).

4.27. The Authority's UAE File Review identified serious and sustained shortcomings in the quality of Due Diligence, particularly in the quality of information collected from customers who presented heightened financial crime risk (and therefore were subject to the requirement for EDD). On the files reviewed, even where SCB's policy required EDD to be applied, frequently only limited EDD measures were carried out which were insufficient given the risks inherent in the business relationships.

Failure to collect adequate customer information

4.28. Throughout the Relevant Period, SCB's internal compliance and monitoring functions of both SCB's Consumer Bank and Wholesale Bank highlighted concerns around the quality of information gathering as part of Due Diligence, with Due Diligence information failing to meet SCB's own standards. This is consistent with evidence the Authority observed in its reviews of customer files.

4.29. From late 2009, numerous internal compliance monitoring reviews identified that customer files in SCB's UAE branches contained inadequate or, in one review, 'scant' information regarding the nature and purpose of customer accounts, and in the case of corporate customers, little detail regarding the nature of the business.

4.30. Two of SCB's compliance monitoring reviews of its UAE branches in 2014 found that the quality of Due Diligence required remediation. One of the reports found that 43% of customer files reviewed did not contain sufficient customer information. Of the files reviewed, 26% failed either to adequately explain the shareholding structure and therefore the beneficial ownership or, in some cases, to identify correctly the authorised signatories and shareholders. Understanding, or 'unwrapping', the shareholder structure is crucial to knowledge of the ultimate beneficial owner and the nature and degree of control that the owner may have

over the customer. These steps form part of a suite of controls firms must use to assist them in assessing whether or not the customer presents any increased risk that SCB could be used for the purposes of money laundering or terrorist financing.

4.31. In February 2012, SCB analysed the practices of unwrapping the ownership structure of corporate entities in its small and medium enterprise customer segment. The analysis revealed that SCB's practice of unwrapping corporate entities was an area of significant risk, including for SCB's UAE branches which had "*gaps*" and Due Diligence which was of poor quality and "*patchy*".

Example of failure to collect sufficient customer information: Customer File A

4.32. This customer exported a dual use good with civil or potential military applications to over 75 countries, including to two jurisdictions where armed conflict was taking place or was likely to be taking place. The customer file did not contain adequate CDD information regarding the purpose of the account, anticipated transaction volumes, or source of funds. The file also lacked documentation to demonstrate that SCB's UAE branches had considered the increased risks around this customer relationship. By its nature, this relationship presented a higher risk of money laundering, terrorist financing or breaching sanctions requirements.

Failure to establish and assess source of funds

4.33. In relation to PEPs, firms must apply on a risk sensitive basis adequate measures to establish the source of wealth and source of funds. SCB's own policies and procedures went further than what was required in the ML Regulations and required SCB's UAE branches to establish the source of funds for a number of other types of customer considered to be higher risk, for example, its small and medium enterprise customers.

4.34. The Authority's UAE File Review in 2014 found failures to establish the legitimacy of funding in high risk customer accounts, for example through establishing the source of funds. The same issue was flagged repeatedly in SCB's own compliance monitoring reviews of its UAE branches throughout the Relevant Period. For example, in December 2009 and September 2010, compliance monitoring reviews of SCB's UAE branches identified that the source of funds information was not adequately explained. An SCB compliance monitoring review in September 2014 of Due Diligence for small and medium enterprise customers also found that in 33% of cases, the information recorded about the customer's source of income and source of funds was insufficient to demonstrate an understanding of the size of the customer's business, its main income streams and the origin of the funds to be received. The poor practice which SCB identified in 2009 therefore persisted in the Consumer Bank, five years later.

Example of source of funds failing: Customer File B

4.35. The customer file for an account opened by a consulate in June 2011 raised serious money laundering concerns. The account was initially funded with a cash deposit of 3m UAE dirhams (AED) (the equivalent of just over £500,000) which the consul had brought into the UAE in a suitcase. The customer file contained little evidence that the source of these funds had been investigated, or whether potential financial crime risk had been considered at account opening. Even where adequate information was gathered, 83% of the Extended Selection files did not *assess* the source of funds information which had been collected at account opening, to determine whether the risk(s) associated with the customer were likely to materialise. Failure to carry out an assessment of source of funds information can lead to money laundering risk not being identified or mitigated.

EDD implementation failures in relation to Iranian nationals

4.36. Banks must apply, on a risk sensitive basis, EDD measures where the risk associated with a business relationship is increased. An understanding of who your customer is and where they come from is crucial to assessing financial crime risk. Whereas SCB's UAE branches had identified an increased financial crime risk in its dealings with Iranian customers, the policies it developed in 2009 and 2010 and the implementation of those policies, while an enhancement to the existing policies, were insufficient in mitigating this risk.

4.37. SCB dealt with Iranian nationals, as long as those customers were resident outside Iran and did not carry out business with/from Iran on their SCB account. In an attempt to manage the heightened financial crime risk of these particular customers, SCB's UAE branches developed the Iran Addendum, a set of eight additional questions to be asked of all Iranian nationals, the purpose of which was to evidence whether the Iranian national genuinely resided outside Iran.

4.38. Historically, UAE branches relied solely on a UAE residence visa as evidence of Iranian national customers not being resident in Iran. By the end of 2009, SCB decided to implement additional measures, as there was a concern that a residency visa might not provide sufficient evidence of an individual's actual residence in the UAE. The Iran Addendum was developed in late 2009 as an additional EDD procedure. It required SCB UAE customers who were Iranian nationals to provide additional information such as frequency of their travel to Iran and the provision of a UAE utility bill in their name. It was circulated to the business on 1 April 2010, to come into effect on 11 April 2010. It was incorporated into SCB policy in October 2010.

4.39. The roll out was poorly managed and incomplete at the outset, and required far more time, adjustments and resource than anticipated. In many cases, branches were unable to obtain the evidence required to establish residency in compliance with the Iran Addendum. The fact that the required evidence could not be obtained led to a significant number of overdue periodic reviews when SCB's UAE branches were required to repeat or supplement the completion of the Iran Addendum due diligence exercise. The backlog ultimately took until 2014 to be significantly remediated.

Deficiencies in Due Diligence: The UK Wholesale Bank's Correspondent Banking business

4.40. In its file review, the Authority found serious and systematic Due Diligence shortcomings in the UK Wholesale Bank's Correspondent Banking business, which had taken place over the CB Relevant Period. These failings were particularly egregious given the high volume and value of SCB's Correspondent Banking transactions during the CB Relevant Period, and the high risk nature of the jurisdictions in which it operated.

Assessment of the Respondent's AML controls and the quality of supervision

4.41. SCB should have carried out an assessment of the quality of the AML controls of the Respondent, including establishing whether these controls met internationally recognised standards. Whilst SCB incorporated the assessment of the quality of a Respondent's supervision in their country risk rating, the Authority's file review found that in 88% of cases, there was insufficient evidence that SCB had assessed adequately the quality of the Respondent's AML controls.

4.42. Whilst the majority of files had some information about the Respondent's AML controls or contained a self-certified AML questionnaire, they did not sufficiently demonstrate that an assessment of the quality of the controls had taken place, nor that SCB had a comprehensive understanding of the effectiveness of the Respondent's AML controls. On 1 December 2010 it had been reported to SCB's Group Financial Crime Risk Committee that there was an *"inadequate assessment of correspondent banking client AML procedures*". The report noted *"apparent 'cut and paste' descriptions of the correspondent's controls*" which *"may be indicative of a tick box approach*".

4.43. Due to the nature of the relationship, the Correspondent is reliant, among other things, on the quality of the Respondent's AML controls. Therefore, the requirement on a Correspondent to assess a Respondent's AML controls is of key importance. By failing to undertake adequately this assessment, SCB was in danger of being unable to determine and understand the risks posed by the Respondent.

Example of Due Diligence failing: Customer File C

4.44. One Respondent was located in a high risk jurisdiction in which armed conflict was taking place at the time of relevant transactions. Despite this, there was no evidence on the file that SCB had obtained, or carried out a qualitative assessment of, the Respondent's AML policies and procedures during the CB Relevant Period. The only relevant evidence on file were standard SCB template AML questionnaires containing yes/no questions about the Respondent's AML controls, and a 'Correspondent Banking Evaluation Sheet' filled in by an SCB employee which contained a single sentence that the Respondent's Due Diligence procedures at account opening and ongoing monitoring were satisfactory. The file did not, for example, reference the fact that the Respondent's parent had previously been the subject of a search and seizure warrant by an overseas law enforcement agency. Where a Correspondent relationship is poorly controlled, it can increase the risk of being used for money laundering or terrorist financing. After SCB ended its relationship with the Respondent, subsequent media reports, denied by the Respondent's group, alleged that members of the Respondent's group had been used by Daesh to fund its organisation. The Authority has not identified evidence to substantiate these reports.

Understanding the nature of the PEP's role in the Respondent

4.45. Correspondents must understand the ownership and management structures of Respondents, including identifying the beneficial owners and/or controllers, and the level of any PEP involvement. By doing so, the Correspondent can secure a better understanding of the risk posed by Respondents. Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. These risks also extend to the members of their immediate families, and to known close associates. PEP status itself does not incriminate individuals or entities. It can, however, increase the level of risk presented by the Respondent.

4.46. Where a PEP has a material beneficial interest or holds a senior management role in a Respondent, firms must take steps to ensure they understand the nature and extent of the PEP's role in the Respondent and the level of control they hold to ensure that the firm has an understanding of the risks. SCB should therefore have undertaken adequate steps to:

a. identify PEPs and whether or not they had any material, beneficial interest or senior management role in the Respondent; and

b. if so, ensure it understood the nature of the PEP's role in the Respondent.

4.47. The Authority's file review found that in 37% of cases SCB had not taken adequate steps to identify PEPs holding a material, beneficial interest or senior management role in the Respondent (for example, by screening significant directors or beneficial owners). For example, the Authority found that, in some cases, there was no evidence screening had taken place at all.

4.48. In 42% of the files where a PEP was identified, there was insufficient evidence that an understanding of the PEP's role in the Respondent had been obtained.

No Due Diligence

4.49. During the CB Relevant Period, SCB did not have any Due Diligence records at all for a small number of the UK Wholesale Bank's non-EEA Correspondent Banking relationships. Although only a small number of relationships were affected, the failure to have any Due Diligence records at all for a relationship is particularly serious as it led to SCB being exposed to increased levels of financial crime risk.

Group Introduction Certificates

4.50. SCB made use of GICs when introducing a customer of one SCB office (the sending office) to another overseas SCB office (the receiving office). Throughout the CB Relevant Period, the Wholesale Bank CDD Policies and Procedures stated that where Due Diligence had already been performed on a customer by another branch or subsidiary within the Standard Chartered Group (i.e. a customer had initially been taken on by another office), it was acceptable, provided a GIC was in place, for that Due Diligence to be used by another overseas branch or subsidiary to open any new, additional accounts for that customer. This was subject to local laws and regulation.

4.51. The GIC ensured, among other things, that:

a. the customer was assigned an appropriate risk rating based on the risk posed to the receiving office. This was important because a customer's risk rating could change as a result of the nature of its relationship with the receiving office. The risk rating had an impact on the extent of the Due Diligence and ongoing monitoring required for that customer; and

b. where there were deficiencies with the Due Diligence undertaken overseas (as was the case in the context of SCB), the GIC process provided the UK Wholesale Bank with an opportunity to review, and where appropriate, highlight inadequate Due Diligence for remediation.

4.52. During the CB Relevant Period, over 75% of the UK Wholesale Bank's non-EEA Correspondent Banking relationships had initially been taken on by an overseas branch or subsidiary and, accordingly, ought to have been subject to GICs. However, as set out in more detail below:

a. SCB did not ensure that a GIC was in place for all of these customers; and

b. even where GICs were in place, SCB did not take sufficient steps to identify deficiencies in the Due Diligence underlying the GICs, in circumstances where SCB was aware that there were issues with the quality of Due Diligence being undertaken overseas.

4.53. In addition, the Authority reviewed a selection of 20 Wholesale Bank customer files that had come from SCB's UAE branch in to SCB's UK office using a GIC. All of those GIC files had been uploaded to SCB's enhanced electronic CDD platform; the Authority therefore expected fewer deficiencies in those files. Despite this remediation, 30% of these GIC files still showed deficiencies in one or more areas.

Absence of GICs

4.54. As noted above, under SCB's own policies, the UK Wholesale Bank could only place reliance on Due Diligence undertaken by an overseas branch or subsidiary in circumstances where a GIC was in place. In breach of the Wholesale Bank CDD Policies and Procedures, 384 (or 29%) of the UK Wholesale Bank's non-EEA Correspondent Banking relationships lacked a GIC into the UK during the CB Relevant Period.

4.55. The UK Wholesale Bank executed just under 400,000 transactions with a total value of approximately $213bn for Correspondent Banking relationships that lacked a GIC into the UK during the period from November 2010 to July 2013 inclusive.

4.56. In circumstances where there was no GIC in place, no separate risk assessment would have been undertaken to determine the level of risk posed by the customer to the UK Wholesale Bank. If this had been done, it would have provided SCB with the opportunity to ensure that any deficiencies in the Due Diligence undertaken by SCB's overseas branches and subsidiaries were rectified when the customer was offered products and services by the UK Wholesale Bank.

Deficiencies in Due Diligence underlying GICs

4.57. Throughout the CB Relevant Period, SCB was aware, from its own group audit reports and compliance monitoring reviews, of various issues with the quality of Due Diligence and ongoing monitoring undertaken by some of its overseas branches and subsidiaries. For example, a November 2010 compliance monitoring review identified inadequacies in the Correspondent Banking Due Diligence undertaken by eight overseas branches and subsidiaries, which were all countries from which the UK Wholesale Bank received GICs.

4.58. Specifically, the review noted inadequate assessments of Respondents' AML controls in the eight overseas branches and subsidiaries, including indications of a tick box approach rather than a proper understanding of the risks. It also noted that GICs were: "*intended to simplify compliance by sharing underlying CDD records. The receiving country depends on the documentation in the core CDD record being correct. Too often they are not"* concluding that as a result of the issues identified: "*Confidence is lost in receiving countries leading to duplication of efforts checking and correcting work. Resources are not in place to do this in a timely fashion, leading to more process problems…*".

4.59. In addition, some of the Due Diligence dispensations granted by SCB to its branches and subsidiaries during the CB Relevant Period meant that they would have been operating at a standard which, in certain circumstances, was lower than that required under the ML Regulations.

4.60. Against this backdrop, SCB failed to take adequate steps to ensure that any deficiencies in the Due Diligence undertaken by SCB's overseas branches and subsidiaries were rectified before the customer was offered products and services by the UK Wholesale Bank.

4.61. The UK Wholesale Bank did not require the receiving office to re-verify the Due Diligence information. However, in practice, the UK Wholesale Bank generally did review the underlying Due Diligence documentation for a Correspondent Banking relationship prior to accepting a GIC from an overseas branch or subsidiary, and on a periodic basis thereafter as part of ongoing monitoring. This review failed to remedy the issues with the Correspondent Banking customer files. All of the files reviewed by the Authority that were subject to a GIC contained one or more of the deficiencies referred to in paragraphs 4.40 to 4.60 above. The UK Wholesale Bank should have identified these deficiencies and refused to accept the customer until those deficiencies had been addressed.

Deficiencies in ongoing monitoring

4.62. The Authority found widespread failures in SCB's reviews of Due Diligence conducted as part of its ongoing monitoring of AML risks from customer accounts. These findings are based on the Authority's UAE File Review, the UK Wholesale Bank's Correspondent Banking files and evidence relating to the poor implementation of the Iran Addendum. Failings were identified in both:

a. periodic reviews in accordance with a customer risk rating, being reviews of Due Diligence materials undertaken after a certain period of time. The time period was determined by the risk rating assigned to the customer; and

b. trigger event reviews, being reviews of Due Diligence materials as a result of a specific trigger event.

4.63. Inadequate or ineffective ongoing monitoring meant SCB could not adequately re-assess the customer relationship as they developed over time, for example where a customer changed its business model, customer base or business ownership. SCB's failure to reassess Due Diligence information and perform adequate ongoing monitoring in a timely manner left it under-informed of money laundering risk.

SCB's UAE branches

4.64. SCB's UAE branches failed to complete periodic reviews in the required timeframes. The Authority's review of customer files identified that there were often long gaps in the periodic review process for high risk customers.

4.65. In addition SCB's UAE branches were reporting significant numbers of overdue periodic reviews for EDD during 2012. For example, in both June and July 2012 there were over 1,700 overdue periodic reviews for EDD customers in the Consumer Bank in SCB's UAE branches. Of those overdue periodic reviews, a significant number related to the inability to complete the Iran Addendum. By October 2012 the proportion of overdue periodic reviews that related to the Iran Addendum was around 43%.

4.66. The Authority identified certain cases where employees in SCB's UAE branches accepted unconvincing information too readily from their customers during ongoing monitoring, in circumstances where there was evidence that to retain the relationship was in breach of SCB's policies. In 2011, concerns were raised within SCB's global investigations function about staff at SCB's UAE branches being more concerned with maintaining client relationships than with complying with financial crime policies.

4.67. The Authority's review of customer files also identified failings relating to the approval of periodic reviews, such as incomplete periodic review forms being approved, or that the appropriate sign-off was not obtained.

4.68. SCB's UAE branches were also required to repeat Due Diligence in response to a number of trigger events, including where:

a. information cast doubt over the veracity or adequacy of documents, data or information previously obtained for CDD purposes;

b. circumstances warranted a review. Such circumstances could include negative press, regulatory/industry notices, or a material change in the beneficial ownership or nature of business; or

c. if a SAR was filed.

4.69. However, SCB's UAE branches did not consistently apply these policies. CDD reviews were not consistently conducted in situations where customers were linked to Rejected Transactions, or where a SAR was reported due to suspicious activity on a customer account. CDD reviews were not performed at all, or where they were performed, were done poorly, too slowly, or did not consider related customer accounts. Weaknesses in SCB's policies and procedures' framework were a contributing factor to these failures.

4.70. SCB's UAE branches' failure to carry out CDD reviews on their customers in accordance with SCB's own policies or adequately identify and assess red flags, such as Rejected Transactions, created the risk that SCB did not sufficiently understand the customer, its business or risk profile. This increased the risk of SCB being used for the purposes of money laundering, terrorist financing or sanctions evasion. In the Extended Selection:

a. 44% of the files that required a review did not contain evidence that a relationship manager carried out a CDD review following a trigger event. A typical trigger event for these customers could include a Rejected Transaction arising in connection with concerns about financial crime risk such as potential links to Iran and/or sanctioned entities; and

b. 80% of customer files containing evidence of a periodic review, did not, however, refer to any of the associated red flags that the Authority identified from its own review. The periodic reviews did not identify instances of Rejected Transactions, cheque payments originating from a sanctioned entity, or payment instructions that were stopped by SCB due to references to Iran.

Example of deficient SCB UAE ongoing monitoring: Customer File D

4.71. This customer opened its account in January 2011. Despite a number of obvious red flags in connection to links with Iran, no CDD review was triggered. The account was exited in September 2011 due to sanctions concerns. The red flags included:

a. clearing the equivalent of $6 million in AED-denominated cheques issued by local branches of Iranian entities in April 2011;

b. blocking a payment instruction to a subsidiary of a sanctioned entity in May 2011; and

c. in July 2011, receiving notifications of Rejected Transactions from another bank on the basis of sanctions on Iran.

4.72. Under SCB's policy, these red flags should have triggered a CDD review.

Example of deficient SCB UAE ongoing monitoring: Customer File E

4.73. This customer opened its account in May 2005, providing a residential address in Tehran but no details of UAE residency. In August 2006 an employee of SCB's UAE branches was informed that the customer was part of an Iranian group of companies that transported oil and derivative products to Iraq via Iran. This information was not included in the customer file.

4.74. In October 2007 and July 2009 there were CDD reviews following a trigger event on the account due to transaction volumes. The reviews identified the customer as a business that had links to a sanctioned country. In May 2010, after a Rejected Transaction due to Iranian sanctions, SCB made a self-disclosure to the US Office of Foreign Assets Control. SCB incorrectly disclosed to the US Office of Foreign Assets Control that the customer had no direct or indirect involvement with Iran and/or a sanctioned entity as SCB thought the customer was operating in the UAE. A CDD review in June 2010, recorded that the customer was not involved in business with links to a sanctioned country, despite earlier and clear indications that it was. It was not until December 2011 that transactions from the account were blocked. The account was eventually exited in June 2012.

Ongoing monitoring: checks under the Iran Addendum

4.75. As part of the Iran Addendum, SCB's UAE branches attempted to introduce a check on the source of payment instructions as part of the Due Diligence review on all accounts where the Iran Addendum applied. The purpose was to ascertain whether payment instructions had been sent by the customer from Iran within the last 12 months. At the time the Iran Addendum was designed and implemented in late 2009 / early 2010, Iran was subject to financial sanctions.

4.76. The additional Due Diligence required a review of a sample of recent payment instructions which included checking whether those instructions came from faxes with the +98 (Iran) country code. The business raised concerns, observing that this additional measure was overly onerous and impractical for staff to complete. As a result this important element of the Iran Addendum was never put into operation. No substitute check replaced it.

4.77. From 2007 to 2012 SCB's UAE branches received, on average, approximately 35,000 faxes per month, which included faxed payment instructions. At its peak, the number of faxed payment instructions received by SCB's UAE branches in a single month from Iran, reached 635 in August 2010. This was a risk which the Iran Addendum would have helped the bank to mitigate. These failures could have been avoided had SCB implemented an effective Iran fax block at the time that the sampling of payment instructions in connection with the Iran Addendum had been proposed.

Ongoing monitoring: The UK Wholesale Bank's Correspondent Banking business

4.78. As at August 2012, SCB had over 3,000 cases of overdue periodic reviews globally, within its Wholesale Bank. Almost half of these related to higher risk accounts that were subject to EDD.

4.79. The Authority found that 72% of the highest risk UK Wholesale Bank Correspondent Banking files had not been reviewed on an annual basis as required under the Wholesale Bank CDD Policies and Procedures.

4.80. This included GIC files, which were subject to periodic reviews by the UK Wholesale Bank, the frequency of which was determined by the risk rating assigned to the

underlying customer. The Authority's file review found that 53% of the highest risk files reviewed that were subject to a GIC had not been reviewed on an annual basis as required by the Wholesale Bank CDD Policies and Procedures.

Deficiencies in oversight of AML risks and controls

4.81. The Authority identified deficiencies in SCB's oversight of AML risks and controls in its UAE branches and its oversight of its Correspondent Banking business in the UK Wholesale Bank. These deficiencies exacerbated the inadequacies identified in SCB's Due Diligence and ongoing monitoring. In particular, SCB failed to:

a. ensure internal checks as part of SCB's first and second lines of defence were effective and provided an appropriate level of scrutiny and challenge in relation to the quality and adequacy of Due Diligence, (paragraphs 4.82 to 4.93);

b. identify and mitigate material financial crime risks in SCB's UAE branches, (paragraphs 4.94 to 4.112); and

c. ensure the escalation of AML risks within SCB was effective, as identified by its group internal audit reports and evident from specific issues which arose in its UAE branches, (paragraphs 4.113 to 4.121).

Ineffective checks as part of SCB's first and second lines of defence

4.82. Throughout the Relevant Period, SCB operated a 'three lines of defence' model for managing financial crime risks.

a. The first line of defence included, among other control measures, regular periodic assessments of a limited sample of customer files, known as KCSAs.

b. Second line of defence measures included the provision of sanctions-related advice by a sanctions advisory function and Due Diligence checks performed by Financial Crime Risk which also conducted compliance monitoring reviews, to evaluate the effectiveness of SCB's controls over particular areas of its business. Financial Crime Risk also set standards and policies for regulatory compliance, and provided advice to SCB's business in relation to these policies. Financial Crime Risk, including SCB's sanctions advisory function, reported in to SCB's Group Head of Compliance.

c. The third line of defence included SCB's group internal audit function which reported to the Standard Chartered Group audit committee.

4.83. The Authority has identified that across SCB's UAE branches and across the UK Wholesale Bank's Correspondent Banking business, there were flaws in the checks carried out by SCB's first and second lines of defence. In addition, in the UAE branches, the second line was overstretched and under-resourced during much of the Relevant Period. This meant that these lines of defence did not act as an effective check on SCB's AML controls. Without robust and challenging first and second lines of defence, SCB exposed itself to an increased risk of being used to further financial crime.

4.84. In October 2011, SCB's UAE branches identified concerns with the quality and capability of certain relationship managers and the CDD they carried out on their customers; a certain account portfolio was "*plagued with account closures due to compliance…*" concerns, which were not investigated. Two employees in SCB's UAE branches had, in fact, colluded with customers in order to evade financial sanctions

against Iran. Other SCB employees in the UAE were aware that accounts were opened for financial sanctions evasion purposes. However, this was not effectively challenged at the time.

KCSAs

4.85. Periodic checks on the completion of Due Diligence were conducted as part of SCB's first line of defence and were applied in both SCB's UAE branches and the UK Wholesale Bank. These checks took the form of a checklist and were known as KCSAs. KCSAs focused on basic administrative checks rather than prompting consideration of the quality and adequacy of Due Diligence.

4.86. The KCSA process for the UK Wholesale Bank as a whole did not provide an appropriate level of scrutiny and challenge in relation to the quality and adequacy of Due Diligence. There were no instances during the CB Relevant Period when the KCSA process identified any issues with Correspondent Banking customer files. This was despite the fact that some files reviewed by the Authority as part of its file review, and found to contain deficiencies, had been subject to KCSAs during the CB Relevant Period.

4.87. Given that the results of KCSAs formed part of the management information that was reported upwards to AML committees within the business and country reporting lines, the inadequacies in the KCSA process gave rise, among other things, to the risk that false comfort would be drawn, and serious weaknesses in SCB's AML controls may have gone unnoticed or not been rectified in a timely manner.

4.88. This risk of 'false comfort' materialised in SCB's oversight of its UAE branches. In 2012, UAE CORC was told that the risk of inadequate Due Diligence on account opening was low. Management information showed that between April and September 2012, the KCSAs were identifying no account opening errors at all in relation to small and medium enterprise customers. However, the Authority's review of customer files and the second line of defence reports in this area identified inadequacies in Due Diligence performed on account opening during this same period.

Financial Crime Risk and Sanctions Advisory functions: resource

4.89. SCB's Financial Crime Risk function in general was under resourced in terms of quantity and quality. In 2010 in SCB's UAE branches, Financial Crime Risk staff were overworked and overloaded. In July 2011 SCB senior management identified that the UAE needed a dedicated advisor for CDD; however, by January 2012 SCB's UAE branches still had limited resource for sanctions and CDD advice. SCB's resourcing outside its UAE branches was also an issue: before the recruitment of additional regional CDD advisors (in 2011) and regional sanctions advisors (in 2012), central resource for advising on CDD and sanctions matters, was severely limited. Despite an increase in resource by July 2014 there remained insufficient resource and a lack of capacity across SCB's Financial Crime Risk and Sanctions Advisory functions.

4.90. There were also deficiencies in the quality of the work done by Financial Crime Risk which played an important role as part of the second line of defence in the UK Wholesale Bank. The Wholesale Bank CDD Policies and Procedures required Financial Crime Risk to review the customer files of all high risk customers, including all Correspondent Banking customer relationships, before the customer was accepted. Financial Crime Risk extended this obligation by carrying out additional checks to perform a substantive qualitative assessment of the customer file (at both the initial acceptance and periodic review stages). However, the quality

of these additional assessments was inadequate and they did not identify all deficiencies in the Due Diligence. The Authority's review of 67 non-EEA Correspondent Banking files found deficiencies in Due Diligence in all of the files; every file had been reviewed by Financial Crime Risk.

Financial Crime Risk: reviews of SCB's UAE branches

4.91. Financial Crime Risk also conducted compliance monitoring reviews, as part of SCB's second line of defence, to evaluate the effectiveness of SCB's controls over particular areas of its business. SCB made no changes to any compliance monitoring policies for its UAE branches to reflect SCB's approval of the Iran Addendum in October 2010. The effect of this was that there was no compliance monitoring conducted at all on the quality of the completion of the Iran Addendum requirements.

4.92. Further, from 2 September 2010 to 30 April 2014 inclusive, a period of three years and eight months, no compliance monitoring reviews relating to Due Diligence or ongoing monitoring were undertaken for the majority of Consumer Bank customers at SCB's UAE branches. For most of the Relevant Period, SCB therefore had little or no information from its compliance function about the adequacy or otherwise of Due Diligence and ongoing monitoring for these customers, except through remediation work.

4.93. In some cases compliance monitoring reviews were scheduled to occur at SCB's UAE branches during this period, but were cancelled or deferred in favour of Financial Crime Risk initiatives including remediation. The decision to defer these reviews was surprising given previous compliance monitoring reviews had identified problems with Due Diligence and ongoing monitoring. For example:

a. in December 2009 a compliance monitoring review observed that the failure to document a customer's source of funds may "*expose the bank to incremental risk, or weaken the bank's ability to monitor actual transactions against anticipated transactions (for that customer account)*", and that the overdue periodic review of EDD customers could "*expos*[e] *the bank to incremental unmanaged risk*"; and

b. a compliance monitoring review report issued on 1 September 2010 further observed that, despite some improvement, the failure in the UAE branches to collect sufficient customer information and to review CDD for previously dormant accounts could lead to a "*weakened AML risk assessment*".

Weaknesses in identifying and mitigating AML risks in its UAE branches

4.94. SCB failed to approach the identification and mitigation of material AML risks in a holistic or proactive manner. In particular it failed to address the risk that its UAE branch customers could access banking services through a variety of channels, including fax and online banking, from countries subject to financial sanctions. Typically, the AML risks which might arise from individuals from countries subject to sanctions accessing banking services include the risks that the bank might be used to transfer the proceeds of crime, including terrorist financing (as well as exposing the bank to breaching sanctions).

Channels access to services: SCB's online banking for retail customers

4.95. In May 2010 during the design of the Iran Addendum the risk that customers in Iran could access SCB's online banking system for retail customers, iBanking, was

noted as something SCB's UAE branches would "*have to live with*". SCB made no attempt to manage the wider implications of this, namely that:

a. this risk was likely to be material and have a global impact, not just an impact on its UAE branches;

b. access to iBanking in its UAE branches could be obtained by customers from other sanctioned countries, not just Iran;

c. access to other online banking channels in its UAE branches, such as its S2B system, could also be exposed to the same risk; and

d. accepting this risk significantly increased the likelihood of SCB breaching sanctions requirements.

4.96. Access to iBanking from sanctioned countries was not completely blocked by SCB until July 2014. This was four years after SCB's UAE branches had first noted the risks posed by customers accessing iBanking from Iran in May 2010.

Channels access to services: SCB's online banking for corporate customers

4.97. The risk of access from sanctioned countries in relation to SCB's online banking system for corporate customers, S2B, was not identified until that risk had crystallised.

4.98. In March 2012, SCB's UAE branches identified that access through S2B had been made from Iran. At this point, SCB's UAE branches considered that the possibility of customers effecting payments from a sanctioned country using the S2B system could be a contravention of its sanctions policy. However, SCB's UAE branches should have realised this in 2010, when the issue of access to its online banking systems from Iran was identified in the context of iBanking when reviewing the Iran Addendum questionnaire. In addition during 2011 SCB dealt with customers with whom it had concerns about links to Iran and in some cases these customers were using, or wanted to use, S2B. This also should have prompted SCB to recognise the risk of S2B being accessed by entities within Iran.

4.99. Having identified this S2B access risk in March 2012, SCB's UAE branches escalated it to senior management and SCB started a bank-wide project to block access and to assess and quantify access via S2B from sanctioned countries. This project blocked most accessibility globally in April 2013, over a year after the customer access to S2B from sanctioned countries became known. Having assessed the numbers of customers who had used S2B from countries subject to sanctions, SCB did not contemporaneously quantify the number and value of transactions that may have resulted from these logins.

Failure to manage access to online banking systems, S2B and iBanking, from within countries subject to financial sanctions

4.100. Attempts to block access to S2B from sanctioned countries became a bank-wide project and were visible to a senior working group in 2012. However, despite the oversight of this working group, governance of the programme was inadequate and the project took too long to reach completion, particularly in the context of SCB's awareness of the risk.

4.101. In June 2012, SCB estimated that the technical solution needed to block S2B access would take between two and three weeks to implement after internal approval was obtained. The two to three week timeframe was restated in September 2012 and

SCB proposed to implement the technical solution as part of a routine update to S2B in the first quarter of 2013. In fact, it was not until 21 April 2013 that the blocks were eventually implemented, over a year after the issue had first been identified in March 2012.

4.102. Reasons for this delay included a failure of governance with initial confusion around which committee or group within SCB was responsible for the resolution of this matter. After the issue was raised before the relevant committee which would ultimately decide to implement the solution in April 2013, SCB's response, focusing on further analysis of the issue, affected customers and technical issues, continued to lack urgency. In March 2013 a failure to progress resolution of the S2B access matter over the prior two months was put down to the issue having "*fallen between the cracks*".

The Iran Addendum

4.103. By November 2009 SCB's UAE branches had identified the risk of customers accessing services in its UAE branches from Iran. The concern that customers might effect payments from a sanctioned country, in this case Iran, and therefore not genuinely residing outside Iran, was considered by SCB to represent a risk to its compliance with sanctions policy. The Iran Addendum, an additional procedure to the EDD process, was designed to mitigate this risk.

4.104. However, even if the Iran Addendum had been effectively implemented and monitored, the procedure was not comprehensive enough to deal with the risks it was supposed to minimise and the general risk of dealing with customers operating from or with Iran. The reasons for this included the following:

a. the Iran Addendum did not cover the risk of UAE branches doing business with customers of other nationalities who were located in Iran. Whilst other CDD measures were in place for identifying customers of other nationalities with links to Iran, there was no comparative measure in place for a customer of different nationality sending payment instructions from Iran.

b. it was only applied to SCB's UAE Consumer Bank and was not used more widely throughout SCB's UAE branches. Therefore it would not, in any event, have covered *all* Iranian national customers of SCB's UAE branches – only those within the Consumer Bank;

c. the payment instruction sampling approach was unlikely to identify non-UAE resident Iranian nationals because the sample sizes of customers' payment instructions proposed to be checked (as described in paragraph 4.75) were too small. Further, it would not have identified any non-UAE resident Iranian nationals who had, for example, simply withheld their originating fax number; and

d. the Iran Addendum required SCB's UAE branches to check the source of payment instructions. The risk of access through iBanking was recognised in SCB's UAE branches in May 2010, just after the Iran Addendum had been initially rolled out. SCB did not adequately explore whether it could check payment instructions made through iBanking, nor did it consider payment instructions sent through S2B. No consideration was given to implementing technological blocks on payment instructions until much later.

4.105. The risk that SCB's services would be accessed from sanctioned countries other than Iran, and through online channels, crystallised and resulted in payments being made throughout the Relevant Period, until SCB implemented the online access

blocks described above. In addition to the volume of faxed payments which appeared to originate from Iran (described at paragraph 4.77 above), payments from SCB's UAE customers that appear to have originated in Iran through online banking systems, with an aggregate value of tens of millions of US dollars, were processed by SCB.

4.106. Each payment exposed SCB to a heightened risk of being used to launder money and/or finance terrorism.

Inadequate response to Rejected Transactions

4.107. Between 2009 and 2011, SCB became aware of a growing number of transactions initiated by customers of SCB's UAE branches being rejected in other jurisdictions, in particular Germany and the United States, due to potential sanctions concerns. SCB's UAE branches did develop some initiatives and perform some specific investigations into customer typologies potentially associated with Rejected Transactions. However, SCB failed to ensure at the time that the UAE branches undertook a comprehensive review of their customer base in response to the heightened sanctions risks indicated by the Rejected Transactions.

4.108. In particular, when the issue was raised to SCB's UAE branches by SCB's New York office in May 2011, SCB's UAE branches did perform periodic reviews that were requested on some of the 18 customers involved in Rejected Transactions. However, SCB's UAE branches did not perform two other reviews that were suggested by SCB's New York office at the same time: one broad review relating to a group of several thousand customers that SCB's New York office considered to pose a high sanctions risk; and one more targeted review relating to a smaller subset of the 30 customers from that population with the most transactions in April 2011. Whilst five of these customers had been previously subject to a periodic review because they had been involved in Rejected Transactions, a periodic review of the remaining 25 customers was never undertaken in response to SCB's New York office's requests, despite repeated requests for information about the status of the reviews.

4.109. Even without the requests from SCB's New York office, the need for a comprehensive review of SCB UAE branches' customer base ought reasonably to have been obvious to SCB from the increasing number of Rejected Transactions, and particularly given that SCB had identified its UAE branches as having a high exposure to the risk of breaching sanctions. However, it was not until February 2012, when SCB held a workshop considering sanctions compliance in two customer segments in the UAE in response to an enquiry by an external agency, that a comprehensive programme was developed and SCB reviewed its relationships with significant numbers of its UAE customers.

4.110. In addition, following the February 2012 workshop, SCB determined that undertaking periodic reviews of customers involved in Rejected Transactions was essential and in May 2012, SCB began work on a protocol (that would also apply to its UAE branches) to provide a consistent model for addressing periodic reviews relating to Rejected Transactions. However, despite repeated escalation of the issue to group level, SCB did not begin to implement the protocol until November 2014, and it was not fully implemented in the UAE until February 2015. This was more than two years after work on the protocol first started. A 2014 group internal audit report noted that the failure to address known capacity issues caused delays in addressing known issues, which included the implementation of the process to review client relationships following a Rejected Transaction.

Inadequate response to warnings about small and medium enterprise CDD

4.111. The UAE branches had a significant number of small and medium enterprise customers. In February 2012, an internal advice memorandum SCB circulated among senior individuals at a group level within SCB's Consumer Bank identified a systemic risk across its Consumer Bank, including in relation to its UAE branches, that the ownership structures of small and medium enterprise customers were not adequately understood to identify the beneficial owners (as described in paragraph 4.31 above). The advice memorandum recommended that potential regulatory, legal and disclosure issues be considered at global or local levels, that further investigation and quantification of unwrapped accounts in the small and medium enterprise and other customer segments should be a top priority, and that urgent CDD remediation take place.

4.112. On learning of this issue the Consumer Bank at a group level decided it "*would treat it as compliance monitoring which has identified a failure in application of policy and procedure, and it will be for countries to determine whether there is a regulatory impact which should be noted through the RRMI* [Regulatory Risk Management Information] *and escalated and tracked through BORC* [Business Operational Risk Committee] *and CORC* [Country Operational Risk Committee]*."* It was only from May 2013, over 14 months after the advice memorandum had been escalated within the Consumer Bank, that SCB implemented measures to improve the quality and consistency of unwrapping. Despite making these changes in May 2013, in September 2014 compliance monitoring reviews in SCB's UAE branches were still identifying issues with small and medium enterprise customers, including in relation to understanding beneficial ownership (as described in paragraph 4.30 above).

Weaknesses in the escalation of AML risks in SCB's UAE branches

4.113. From before the commencement of the Relevant Period, up to at least September 2013, SCB failed adequately to escalate AML risks, or to ensure adequate governance over the management of those risks.

4.114. SCB failed effectively to identify and escalate:

a. material financial crime risks identified in its UAE branches relating to Due Diligence and ongoing monitoring; and

b. the decision not to implement the proposed check on payment instructions of the Iran Addendum, which had a significant detrimental impact on the ability of SCB to ensure its branches conducted effective EDD on customers presenting a higher AML risk.

Concerns over escalation known to SCB

4.115. Inadequacies in SCB's escalation of AML risks were identified and raised by SCB's group internal audit function:

a. In August 2008 SCB's group internal audit function graded the oversight and management of AML risks at group level in relation to Consumer Bank customers as "*Fail*". The report stated that a "*review of the CB FCR* [Consumer Banking Financial Crime Risk] *Committee meeting minutes as of the date of the audit did not show evidence of country specific AML issues being escalated to the committee although Group Internal Audit (GIA) has found several significant risk issues during BAU* [Business As Usual] *product audits*";

b. When CDD / AML issues were increasingly highlighted in group internal audits up to June 2010, the need for a "*Much tighter focus and follow up by Senior Management and the Governance Committees on Anti-Money Laundering Management Information*" was identified, with group internal audit noting that it would conduct an AML themed audit later in 2010 focusing on countries that were reporting high levels of CDD errors and overdue periodic reviews to determine the root cause of the issue;

c. In March 2011 a group internal audit report identified that, during 2010, management information about the non-performance of trigger event reviews after filing SARs (described further in paragraph 4.69 above) within the Consumer Bank in SCB's UAE branches, was not being escalated correctly. The report noted that "*lack of adequate escalation of KCSA exceptions on SARs may lead to instances where potential AML and CDD gaps are not rectified in a timely manner*";

d. In December 2012 a group internal audit report identified that problems with management information could lead to the risk that matters which merited escalation may not be escalated. The report mentioned, in particular, the transparency of management information concerning the number of customers that lacked, or had inadequate, CDD and recorded the risk that: "*Committee decisions, the degree of escalation and general management attention may not remain proportionate to the level of risk*";

e. Concerns were raised in another group internal audit report in June 2013 about poor status reporting, identifying the consequence that this could lead to poor escalation; and

f. By September 2013 group internal audit were still raising concerns about SCB's AML risk governance management across group, business and country levels. While overall the report was graded "*Acceptable*", it also identified that escalation of AML issues and risks to SCB's risk committee and Standard Chartered Group's audit committee was inconsistent. The report stated that "[t]*here is no visible audit trail of how material AML issues from Country FCR* [Financial Crime Risk] *to Group FCR are escalated. Whilst issues and risks are escalated effectively between the lower levels, the criteria for escalating issues from Group FCR to the next level, i.e. to* [sic] *GFCR to GRC* [Group Risk Committee]*, is unclear. This is reflective of a wider absence of detailed escalation criteria across the function. The root cause of this is there is no clear or transparent mechanism that allows issues to be escalated in a consistent method to the Board Committees.*"

Failure to escalate Due Diligence and ongoing monitoring issues in the Consumer Bank in SCB's UAE branches

4.116. Material financial crime risks and issues relating to Due Diligence and ongoing monitoring identified in the Consumer Bank in SCB's UAE branches were not escalated to SCB GORC in accordance with SCB's policy.

4.117. In particular, in March 2012, SCB's UAE CORC recognised that SCB risked breaching regulatory requirements by not carrying out Due Diligence or periodic reviews properly and in accordance with its own policies and procedures. The grading of the risk was considered high by UAE CORC and therefore should have been escalated according to SCB's own policies. However, despite UAE CORC considering the risk to be high for eight months, this risk was never escalated to SCB GORC.

Failure to escalate breaches of Due Diligence policy regarding Iranian nationals

4.118. The decision not to implement one of the key elements of the Iran Addendum, the requirement to ascertain whether payment instructions had been sent by customers located in Iran, including by fax, was never escalated.

4.119. The non-implementation of this should have been categorised as a high risk according to SCB's own operational risk framework because the impact to the group of not implementing the policy was to expose the UAE branches to the material risk that customers were sending payment instructions from Iran by fax. This matter and the risks it gave rise to were not escalated for consideration by any senior level committees, either at country level or group level.

4.120. If this escalation had occurred, senior committees would have been able to consider and address risks arising from the non-implementation. The importance of ensuring adequate oversight of SCB's UAE branches was demonstrated by the penalties imposed on SCB by US authorities in September and December 2012. The penalties related to misconduct in its UAE branches, specifically the removal or omission of Iranian information from US dollar wire payment messages, among other things. During 2001 to 2007 approximately $3.9bn of non-transparent Iranian transactions were sent from SCB's UAE branches through SCB's New York branch on behalf of Iranian-owned banks, corporations and other unknown entities. US authorities referred to inadequate controls in SCB's UAE branches as contributing to the breaches identified.

4.121. It was not until February 2014, after enquiries from US agencies in late 2013, that SCB began investigating the scope of faxed payment instructions into the UAE from Iran. Only by mid to late 2014 had SCB implemented technological blocks in the UAE regarding faxes and telephone calls.

Remedial steps taken by SCB

4.122. SCB is working with the Authority as well as other regulators in various jurisdictions in which it operates to improve its AML controls. As part of this, SCB is instituting a range of measures designed to improve its governance structure and oversight of its non-EEA branches and subsidiaries.

4.123. Steps taken by SCB include the following:

a. during the Relevant Period SCB reviewed and updated its Due Diligence policies and procedures;

b. SCB has invested significant resource to improve the underlying quality of its Due Diligence. This included the introduction of a new electronic CDD platform, known as eCDD+, in 2012. However, the introduction of the eCDD+ system was complex, leading to a significant backlog of periodic reviews during the latter part of the Relevant Period. SCB's group internal audit also identified project governance weaknesses with this Due Diligence remediation project, which SCB's group internal audit noted had temporarily impacted business operations at an unacceptable level. SCB committed significant resource to clear the periodic review backlog, and to remediate the Due Diligence control environment as a whole;

c. SCB has significantly increased the resource dedicated to managing financial crime risk. The number of AML professionals employed by SCB has approximately quadrupled since the end of 2012. SCB has also made key

strategic appointments in senior roles, including appointing a new Global Head of Financial Crime Compliance;

d. SCB has taken steps to strengthen governance of financial crime risk, including in relation to its Correspondent Banking Due Diligence practices and its Due Diligence and ongoing monitoring in its UAE branches. In particular, in 2013 SCB developed and introduced an integrated financial crime risk strategy, which included an explicit strategic objective for financial crime. In 2015, SCB established a Board Financial Crime Risk Committee, responsible for overseeing the effectiveness of Standard Chartered Group's policies, procedures, systems, controls and assurance arrangements relating to financial crime risk. It also created Country Financial Crime Risk Committees in various jurisdictions, including the UK and the UAE;

e. SCB has introduced new quality assurance checks to replace and/or supplement KCSAs;

f. since the end of the Relevant Period, SCB has taken steps to identify, validate and remediate (as appropriate) any GIC gaps;

g. in 2014, SCB introduced new committees to improve oversight of SCB's Correspondent Banking business, including a Correspondent Banking Working Committee and Correspondent Banking Oversight Committee;

h. in 2015, SCB launched a Financial Crime Compliance Correspondent Banking Academy. The Academy offers AML and sanctions training to SCB's respondent bank customers (especially in high-risk jurisdictions with significant transaction volumes), with the aim of strengthening its AML controls; and

i. SCB has agreed with the Authority to take the matters set out in this Notice into account, in accordance with the Remuneration Code in the Handbook, in the next bonus and vesting decisions to be made by SCB and to confirm to the Authority how this has been done.

5. FAILINGS

5.1. The statutory and regulatory provisions relevant to this Notice are set out in Annex A.

5.2. On the basis of the facts and matters set out above, the Authority considers that SCB breached:

a. ML Regulation 14(3), as SCB failed during the CB Relevant Period to ensure that the UK Wholesale Bank carried out adequate enhanced due diligence and ongoing monitoring of its Respondents from non-EEA states;

b. ML Regulation 15(1), as SCB did not require its UAE branches to apply measures at least equivalent to those set out in the ML Regulations with regard to customer due diligence and ongoing monitoring; and

c. ML Regulation 20(1), as SCB did not establish and maintain appropriate and risk-sensitive AML policies and procedures, or ensure that all aspects of its AML policies and procedures were applied appropriately and consistently in respect of its UAE branches and the UK Wholesale Bank's Correspondent Banking relationships during the Relevant Period and CB Relevant Period respectively.

Deficiencies in AML controls

5.3. As well as Regulations 14(3), 15(1) and 20(1), SCB's conduct failed to comply with Regulations 7(1) to (3), 8(1) and (3) and 14(4) of the ML Regulations.

Deficiencies in Due Diligence

5.4. SCB failed to require its UAE branches to apply measures at least equivalent to those set out in the ML Regulations with regard to Due Diligence. Both SCB's own monitoring and the file reviews conducted by the Authority show failures in collecting and analysing customer information and in consistently establishing the source of funds. Requiring its UAE branches to have adequate Due Diligence controls was particularly important given that SCB had identified enhanced risks of financial crime in its UAE branches and had instituted, or attempted to institute, particular policies to deal with these enhanced risks. The roll out of the Iran Addendum was poor and, although the Iran Addendum was an enhancement to reduce the risk of SCB UAE banking Iranian nationals purporting to be resident in the UAE, it did not sufficiently mitigate the risks identified by SCB.

5.5. SCB failed to ensure an appropriate level of Due Diligence in its Correspondent Banking relationships in the UK Wholesale Bank. The Authority considers SCB's failure adequately to undertake an assessment of the Respondent's AML controls to be particularly serious, as it risked compromising SCB's ability to manage the financial crime risk associated with these relationships.

Deficiencies in ongoing monitoring

5.6. There were failures in SCB's ongoing monitoring in relation to customers of its UAE branches and to the UK Wholesale Bank's Correspondent Banking relationships. In particular, SCB failed to ensure that its UAE branches promptly and consistently performed periodic reviews, and the failure to implement the proposed sample check of payment instructions under the Iran Addendum, or to develop alternative measures, meant the financial crime risk to SCB was significantly increased. SCB processed a significant volume of payments where instructions originated in countries subject to sanctions. There were also failures around conducting periodic reviews in response to trigger events.

5.7. Failures to conduct timely periodic reviews also occurred in the UK Wholesale Bank's Correspondent Bank where, of the highest risk files, 72% had not been reviewed on an annual basis.

5.8. In its file reviews, the Authority observed shortcomings in the application of SCB's Due Diligence policies and procedures. This suggests, among other things, that relevant staff did not have a sufficient understanding of what was required of them under those policies and procedures. It therefore appears that SCB failed to ensure that all employees involved in the production and review of Due Diligence received adequate training. The Authority perceives this to be a contributing factor to the deficiencies identified.

Deficiencies in oversight of AML controls

5.9. SCB's oversight of its AML controls in its UAE branches and the UK Wholesale Bank's Correspondent Banking business was insufficiently robust. In particular, in the UAE branches, there was evidence of collusion to evade controls and knowledge by UAE employees of accounts operated for financial sanctions evasion. Effective oversight, checks and controls would have encouraged and assisted in embedding a positive AML culture and minimised opportunities for evasion.

Inadequacies in SCB's first and second lines of defence

5.10. The deficiencies observed by the Authority in its review of the UK Wholesale Bank's Correspondent Banking files where KCSAs had been completed, indicated that the KCSA process was deficient. In particular, the KCSA check itself focused on administrative checks and was inadequate to test the *quality* of the Due Diligence.

5.11. Financial Crime Risk played a key role in SCB's second line of defence. However, particularly in the early part of the Relevant Period, the quality and quantity of resource in this area was inadequate. When coupled with the absence of compliance monitoring reviews completed by Financial Crime Risk of SCB's UAE branches for a period of over 3.5 years, the deficiencies in the first and second lines of defence meant that SCB had inadequate oversight of AML controls in its UK Wholesale Bank's Correspondent Banking business and its Consumer Bank in its UAE branches.

Weaknesses in identifying and mitigating material AML risks

5.12. SCB's approach to identifying and mitigating the following material AML risks in its UAE branches was narrow, slow and consistent with a reactive, rather than a proactive, approach to financial crime risk.

5.13. It failed to identify and mitigate promptly the risk that customers could use a *variety* of access points to issue payment instructions from countries subject to sanctions and the measures it put in place, for example the Iran Addendum, were inadequate to mitigate the risk. Oversight and governance of the project coordinating the blocking of online access was similarly deficient. This was despite oversight by a senior working group with insight into the risk being run whilst blocks were not in place, and an understanding that effecting the blocks would take a matter of weeks. SCB's response to Rejected Transactions was inadequate, and it took nearly one and a half years to respond to risks raised about the inadequacy of understanding of the beneficial ownership of its small and medium enterprise customers.

5.14. It appears that, in these instances, financial crime risk was not adequately prioritised and when implementing the Iran Addendum SCB failed to act on the evident risks of allowing its payments systems to be used by those subject to sanctions.

Weaknesses in the escalation of AML risks

5.15. There were weaknesses in the escalation of AML risks, in particular concerning SCB's UAE branches, from country to group and board level throughout the Relevant Period. These escalation weaknesses were identified by SCB's internal audit which also recognised that these weaknesses restricted the ability of SCB to exercise adequate oversight of its AML controls.

Culture

5.16. The facts and matters in this notice give rise to the concern that, in particular in relation to its operations in the UAE, SCB failed to take reasonable steps to ensure a positive culture towards AML compliance was embedded particularly during the early part of the Relevant Period. This concern arises principally from the resourcing constraints within Financial Crime Risk, employees in the UAE branches colluding to evade controls and knowledge by other UAE employees of accounts operated for financial sanctions evasion, as well as a lack of urgency in resolving

the technical blocks for S2B access, and a failure to take a holistic approach towards financial crime controls.

Serious nature of the failings

5.17. The weaknesses in SCB's AML systems and controls resulted in an unacceptable risk that SCB would be used by those seeking to launder money, evade financial sanctions or finance terrorism.

5.18. The Authority considers SCB's failings to be particularly serious because these failures occurred against the following backdrop:

a. Industry-wide messaging specifically highlighting jurisdictions with a high risk of money laundering and/or financial crime. Throughout the Relevant Period, the UK government as well as international and domestic governmental organisations repeatedly issued communications regarding jurisdictions with a high risk of money laundering and/or financial crime. This included Iran which, by virtue of its geographical proximity and historic ties between the two countries, presented additional challenges for SCB's UAE branches in relation to their Due Diligence and ongoing monitoring, as well as for SCB more widely in terms of its oversight of the controls within the UAE branches;

b. relevant publications and guidance by the Authority in which it stressed the importance of maintaining appropriate financial crime controls:

i. during the Relevant Period, the Authority took enforcement action against a number of authorised firms for failings relating to financial crime. These actions covered similar themes to the failings identified by the Authority in the context of its investigation into SCB, including the need to ensure that financial crime controls were adequate for higher risk customers, including Correspondent Banking relationships, as well as to prevent sanctions evasion. The Authority published details of its actions; and

ii. as well as publishing various thematic reviews both before and during the Relevant Period, in December 2011 the Authority published consolidated guidance on financial crime, to help firms adopt a more effective approach to mitigating financial crime risk. The guidance emphasised the need to conduct adequate customer Due Diligence checks, to perform ongoing monitoring, and, when handling higher risk situations such as Correspondent Banking relationships, to undertake enhanced due diligence and enhanced ongoing monitoring. This guidance has been regularly updated since;

c. direct feedback from the Authority to SCB in 2010 and 2013:

i. the Authority gave feedback to SCB following a thematic review visit to SCB's London office in November 2010. The Authority's feedback concluded that the Authority remained concerned that AML risks relating to PEPs and Correspondent Banking might not be being properly managed and that these weaknesses might be replicated in SCB's business undertaken outside the UK. As part of the feedback, SCB was asked by the Authority to consider what additional steps it should take to assess these risks and to put in place appropriate remedial action as a matter of urgency; and

ii. feedback provided by the Authority following a SAMLP assessment of AML and sanctions controls in 2013 which highlighted a number of weaknesses in sanctions controls; and

d. relevant action taken by US authorities in 2012 in relation to 'wire stripping' i.e. the removal or omission of Iranian information from US dollar wire payment messages in the period from 2002 to 2007 inclusive. Further action relating to SCB's financial crime controls was taken by the US authorities in late 2014. By July 2014, SCB had decided to exit its business with most small and medium enterprise customers in its UAE branches. The bank's decision was then included as a requirement in the US action in August 2014.

5.19. Firms with weak financial crime controls may have an unfair competitive advantage over firms competing in the same sector, in that they may be able to take on customers that other firms - with robust financial crime controls - would be obliged to turn away. Effective enforcement action provides a significant disincentive to non-compliance with legal and regulatory requirements, and enables firms to compete in legitimate ways, to the benefit of consumers.

6. SANCTION

6.1. Pursuant to Regulations 36(a) and 42(1) of the ML Regulations, the Authority is a designated authority who may impose a penalty on a relevant person for failure to comply with the ML Regulations at issue in this Notice.

6.2. SCB is a relevant person pursuant to Regulations 3(2) and 3(3) of the ML Regulations.

6.3. In deciding whether SCB has failed to comply with the relevant requirements of the ML Regulations, the Authority has considered whether SCB followed the relevant JMLSG Guidance as the JMLSG Guidance meets the requirements set out in Regulation 42(3) of the ML Regulations (being guidance approved by the Treasury).

6.4. In accordance with Regulation 42(2) of the ML Regulations, the Authority has considered whether it can be satisfied that SCB took all reasonable steps and exercised all due diligence to ensure that the requirements of the ML Regulations would be complied with. The Authority has concluded that it cannot for the reasons set out in Section 5 of this Notice. The Authority considers that an element of SCB's conduct during the Relevant Period indicates that SCB failed to act on the evident risks of allowing its payments systems to be used by those subject to sanctions.

6.5. Regulation 42(1) of the ML Regulations states that the Authority may impose a penalty of such amount as it considers appropriate on a relevant person for failure to comply with the ML Regulations at issue in this Notice.

6.6. The Authority has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.

6.7. During the Relevant Period, paragraph 19.15.5 of the Enforcement Guide stated that, when imposing or determining the level of a financial penalty under the ML Regulations, the Authority's policy includes having regard, where relevant, to relevant factors in DEPP 6.2.1G and DEPP 6.5 to DEPP 6.5D.

6.8. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. On 6 March 2010, the Authority's new penalty framework came into force. SCB's misconduct covers a period across 6 March 2010. However, the Authority considers that most of SCB's misconduct occurred after 6 March 2010. The

Authority has therefore assessed the financial penalty under the regime in force on 6 March 2010.

6.9. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

6.10. The application of the Authority's penalty policy in relation to the failings noted in Section 5 is set out in Annex B to this Notice. Having regard to all the circumstances, the Authority considers that £145,947,500 (£102,163,200 after 30% (stage 1) discount) is the appropriate financial penalty to impose on SCB. Of the penalty, £123,317,600 (£86,322,300 after 30% (stage 1) discount) relates to failings in SCB's oversight of its UAE branches, and £22,629,800 (£15,840,900 after 30% (stage 1) discount) relates to SCB's Correspondent Banking failings.

7. REPRESENTATIONS

7.1. Annex C contains a brief summary of the key representations made by SCB and how they have been dealt with. As SCB agreed to settle in relation to all relevant facts and all issues as to whether those facts constitute breaches, SCB only made representations on the proposed financial penalty. In making the decision which gave rise to the obligation to give this Notice, the Authority has taken into account all of the representations made by SCB, whether or not set out in Annex C.

8. PROCEDURAL MATTERS

8.1. This Notice is given in accordance with Regulation 42(7) of the ML Regulations. The following information is important.

Decision maker

8.2. The decision which gave rise to the obligation to give this Notice was made by the Regulatory Decisions Committee.

The Tribunal

8.3. SCB has the right to appeal the decision to impose a penalty to the Tribunal. The Tax and Chancery Chamber is the part of the Upper Tribunal which, among other things, hears appeals arising from decisions of the Authority. Under paragraph 2(2) of Schedule 3 to the Tribunal Procedure (Upper Tribunal) Rules 2008, SCB has 28 days from the date on which this Notice is given to SCB to refer the appeal to the Tribunal.

8.4. An appeal to the Tribunal is made by way of a signed reference notice (Form FTC3) filed with a copy of this Notice. The Tribunal's contact details are: Upper Tribunal, (Tax and Chancery Chamber), Fifth Floor, Rolls Building, Fetter Lane, London, EC4A 1NL (tel: 020 7612 9730; email: fs@hmcts.gsi.gov.uk.

8.5. Further information on the Tribunal, including a link to 'Forms and leaflets' which include Form FTC3 and notes on that form, can be found on the HM Courts and Tribunals website:

https://www.justice.gov.uk/tribunals/tax-and-chancery-upper-tribunal

8.6. A copy of Form FTC3 must also be sent to Bill Sillett at the Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN at the same time as filing a reference with the Upper Tribunal.

Access to evidence

8.7. The Authority grants to the person to whom this Notice is given access to:

a. the material upon which the Authority has relied on in deciding to give this Notice; and

b. the secondary material which, in the opinion of the Authority, might undermine that decision.

Third party rights

8.8. No third party rights apply in respect of this notice.

Confidentiality and publicity

8.9. This Notice may contain confidential information and should not be disclosed to a third party (except for the purpose of obtaining advice on its contents).

8.10. However, the Authority will publish such information about the matter to which this Notice relates as it considers appropriate.

Contacts

8.11. For more information concerning this matter generally, contact Bill Sillett (direct line: 020 7066 5880) of the Enforcement and Market Oversight Division of the Authority.

Tim Parkes
Chair, Regulatory Decisions Committee

ANNEX A - RELEVANT STATUTORY AND REGULATORY PROVISIONS AND GUIDANCE

The Money Laundering Regulations 2007 were in force from 15 December 2007 to 25 June 2017 inclusive and have been repealed and replaced by the Money Laundering Regulations 2017, which came into force on 26 June 2017. In this Notice, the Authority refers to and has taken action under the Money Laundering Regulations 2007 as the Relevant Period occurred when the Money Laundering Regulations 2007 were in force.

Relevant extracts from the Money Laundering Regulations 2007

Meaning of customer due diligence measures

1. Regulation 5 states:

> *"Customer due diligence measures" means—*
>
> *(a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;*
>
> *(b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and*
>
> *(c) obtaining information on the purpose and intended nature of the business relationship.*

Meaning of beneficial owner

2. Regulation 6 states:

> *(1) In the case of a body corporate, "beneficial owner" means any individual who—*
>
> *(a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or*
>
> *(b) as respects any body corporate, otherwise exercises control over the management of the body.*
>
> *(2) In the case of a partnership (other than a limited liability partnership), "beneficial owner" means any individual who—*
>
> *(a) ultimately is entitled to or controls (whether the entitlement or control is direct or indirect) more than a 25% share of the capital or profits of the partnership or more than 25% of the voting rights in the partnership; or*
>
> *(b) otherwise exercises control over the management of the partnership. […]*

Application of customer due diligence measures

3. Regulation 7 states:

(1) Subject to regulations 9, 10, 12, 13, 14, 16(4) and 17, a relevant person must apply customer due diligence measures when he—

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

(3) A relevant person must—

(a) determine the extent of customer due diligence measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction; and

(b) be able to demonstrate to his supervisory authority that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing. […]

Ongoing monitoring

4. Regulation 8 states:

(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means—

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures.

Enhanced customer due diligence and ongoing monitoring

5. Regulation 14 states:

(1) A relevant person must apply on a risk sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring –

(a) In accordance with paragraphs (2) to (4);

(b) In any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

(3) A credit institution ("the correspondent") which has or proposes to have a correspondent banking relationship with a respondent institution ("the respondent") from a non-EEA state must—

(a) gather sufficient information about the respondent to understand fully the nature of its business;

(b) determine from publicly-available information the reputation of the respondent and the quality of its supervision;

(c) assess the respondent's anti-money laundering and anti-terrorist financing controls;

(d) obtain approval from senior management before establishing a new correspondent banking relationship;

(e) document the respective responsibilities of the respondent and correspondent; and

(f) be satisfied that, in respect of those of the respondent's customers who have direct access to accounts of the correspondent, the respondent—

(i) has verified the identity of, and conducts ongoing monitoring in respect of, such customers; and

(ii) is able to provide to the correspondent, upon request, the documents, data or information obtained when applying customer due diligence measures and ongoing monitoring.

(4) A relevant person who proposes to have a business relationship or carry out an occasional transaction with a politically exposed person must—

(a) have approval from senior management for establishing the business relationship with that person;

(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or occasional transaction; and

(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

(5) In paragraph (4), "a politically exposed person" means a person who is—

(a) an individual who is or has, at any time in the preceding year, been entrusted with a prominent public function by—

(i) a state other than the United Kingdom;

(ii) a Community institution; or

(iii) an international body,

including a person who falls in any of the categories listed in paragraph 4(1)(a) of Schedule 2;

(b) an immediate family member of a person referred to in sub-paragraph (a), including a person who falls in any of the categories listed in paragraph 4(1)(c) of Schedule 2; or

(c) a known close associate of a person referred to in sub-paragraph (a), including a person who falls in either of the categories listed in paragraph 4(1)(d) of Schedule 2.

(6) For the purpose of deciding whether a person is a known close associate of a person referred to in paragraph (5)(a), a relevant person need only have regard to information which is in his possession or is publicly known.

Branches and subsidiaries

6. Regulation 15 states:

(1) A credit or financial institution must require its branches and subsidiary undertakings which are located in a non-EEA state to apply, to the extent permitted by the law of that state, measures at least equivalent to those set out in these Regulations with regard to customer due diligence measures, ongoing monitoring and record-keeping.

Reliance

7. Regulation 17 states:

(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

Policies and procedures

8. Regulation 20 states:

(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to-

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures-

(a) which provide for the identification and scrutiny of- […]

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;

(b) which specify the taking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products and transactions which might favour anonymity;

(c) to determine whether a customer is a politically exposed person; […]

(5) A credit or financial institution must communicate where relevant the policies and procedures which it establishes and maintains in accordance with this regulation to its branches and subsidiary undertakings which are located outside the United Kingdom.

Relevant extracts from the JMLSG Guidance

9. The JMLSG Guidance provisions set out below are taken from the November 2009 version of the guidance. The JMLSG Guidance is periodically updated, however, there were no material changes to the provisions set out below during the Relevant Period.

Part I, Chapter 1 Senior Management Responsibility

Application of group policies outside the UK

10. Paragraph 1.44 states:

The UK legal and regulatory regime is primarily concerned with preventing money laundering which is connected with the UK. Where a UK financial institution has overseas branches, subsidiaries or associates, where control can be exercised over business carried on outside the United Kingdom, or where elements of its UK business have been outsourced to offshore locations (see paragraphs 2.7-2.11), the firm must put in place a group AML/CTF strategy.

11. Paragraph 1.45 states:

A group policy must ensure that all non-EEA branches and subsidiaries carry out CDD measures, and keep records, at least to the standards required under UK law

or, if the standards in the host country are more rigorous, to those higher standards. Reporting processes must nevertheless follow local laws and procedures.

Part I, Chapter 2 Internal Controls

General legal and regulatory obligations

12. Paragraph 2.1 states:

There is a requirement for firms to establish and maintain appropriate and risk-based policies and procedures in order to prevent operations related to money laundering or terrorist financing. FSA-regulated firms have similar, regulatory obligations under SYSC.

Part I, Chapter 3 Nominated Officer / Money Laundering Reporting Officer (MLRO)

Monitoring effectiveness of money laundering controls

13. Paragraph 3.27 states:

A firm is required to carry out regular assessments of the adequacy of its systems and controls to ensure that they manage the money laundering risk effectively. Oversight of the implementation of the firm's AML/CTF policies and procedures, including the operation of the risk-based approach, is the responsibility of the MLRO, under delegation from senior management. He must therefore ensure that appropriate monitoring processes and procedures across the firm are established and maintained.

Part I, Chapter 5 Customer Due Diligence

Meaning of customer due diligence measures and ongoing monitoring

14. Paragraph 5.1.4 states:

Firms must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. They must be able to demonstrate to their supervisory authority that the extent of their CDD measures and monitoring is appropriate in view of the risks of money laundering and terrorist financing.

15. Paragraph 5.1.6 states:

Where the customer is a legal person (such as a company) or a legal arrangement (such as a trust), part of the obligation on firms to identify any beneficial owner of the customer means firms taking measures to understand the ownership and control structure of the customer.

16. Paragraph 5.1.10 states:

The CDD and monitoring obligations on firms under legislation and regulation are designed to make it more difficult for the financial services industry to be used for money laundering or terrorist financing.

17. Paragraph 5.1.11 states:

Firms also need to know who their customers are to guard against fraud, including impersonation fraud, and the risk of committing offences under POCA and the Terrorism Act, relating to money laundering and terrorist financing.

18. Paragraph 5.1.12 states:

Firms therefore need to carry out customer due diligence, and monitoring, for two broad reasons:

- *to help the firm, at the time due diligence is carried out, to be reasonably satisfied that customers are who they say they are, to know whether they are acting on behalf of another, and that there is no legal barrier (e.g. government sanctions) to providing them with the product or service requested; and*

- *to enable the firm to assist law enforcement, by providing available information on customers or activities being investigated.*

19. Paragraph 5.1.13 states:

It may often be appropriate for the firm to know rather more about the customer than his identity: it will, for example, often need to be aware of the nature of the customer's business in order to assess the extent to which his transactions and activity undertaken with or through the firm is consistent with that business.

Application of CDD measures

20. Paragraph 5.3.1 states:

Applying CDD measures involves several steps. The firm is required to verify the identity of customers and, where applicable, beneficial owners. Information on the purpose and intended nature of the business relationship must also be obtained.

Enhanced due diligence

21. Paragraph 5.5.1 states:

A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the standard evidence of identity is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer.

22. Paragraph 5.5.2 states:

As a part of a risk-based approach, therefore, firms may need to hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons:

- *to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and*

- *to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.*

23. Paragraph 5.5.5 states:

A firm should hold a fuller set of information in respect of those customers, or class/category of customers, assessed as carrying a higher money laundering or terrorist financing risk, or who are seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.

24. Paragraph 5.5.18 states:

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates. PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.

25. Paragraph 5.5.25 states:

Firms are required, on a risk-sensitive basis, to:

a. *have appropriate risk-based procedures to determine whether a customer is a PEP;*
b. *obtain appropriate senior management approval for establishing a business relationship with such a customer;*
c. *take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship or occasional transaction; and*
d. *conduct enhanced ongoing monitoring of the business relationship.*

26. Paragraph 5.6.26 states:

Where a customer is introduced by one part of a financial sector group to another, it is not necessary for his identity to be re-verified, provided that:

a. *the identity of the customer has been verified by the introducing part of the group in line with AML/CTF standards in the UK, the EU or an equivalent jurisdiction; and*
b. *the group entity that carried out the CDD measures can be relied upon as a third party under Regulation 17(2).*

Monitoring customer activity

27. Paragraph 5.7.1 states:

Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- *Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;*

- *Ensuring that the documents, data or information held by the firm are kept up to date.*

28. Paragraph 5.7.2 states:

Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

29. Paragraph 5.7.12 states:

Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

***Part I, Chapter 7* Staff awareness, training and alertness**

Why focus on staff awareness and training?

30. Paragraph 7.1 states:

One of the most important controls over the prevention and detection of money laundering is to have staff who are alert to the risks of money laundering/terrorist financing and well trained in the identification of unusual activities or transactions which may prove to be suspicious.

31. Paragraph 7.2 states:

The effective application of even the best designed control systems can be quickly compromised if the staff applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the firm's AML/CTF strategy.

Part II, Chapter 16 Correspondent banking

Overview of the sector

32. Paragraph 16.1 states:

For the purposes of this guidance, correspondent banking is defined as the provision of banking-related services by one bank (Correspondent) to an overseas bank (Respondent) to enable the Respondent to provide its own customers with cross-border products and services that it cannot provide them with itself, typically due to a lack of an international network.

How to assess the elements of risk in correspondent banking

33. Paragraph 16.9 states:

Enhanced customer due diligence (see Part I, section 5.5) must be undertaken on Respondents (and/or third parties authorised exceptionally to provide instructions to the Correspondent e.g., other entities within a Respondent group) using a risk-based approach. The following risk indicators should be considered both when initiating a relationship, and on a continuing basis thereafter, to determine the levels of risk-based due diligence that should be undertaken:

- ***The Respondent's domicile.*** *The jurisdiction where the Respondent is based and/or where its ultimate parent is headquartered may present*

greater risk (or may mitigate the risk, depending on the circumstances). Certain jurisdictions are recognised internationally as having inadequate anti-money laundering standards, insufficient regulatory supervision, or presenting greater risk for crime, corruption or terrorist financing. Other jurisdictions, however, such as many members of the Financial Action Task Force (FATF), have more robust regulatory environments, representing lower risks. Correspondents should review pronouncements from regulatory agencies and international bodies such as the FATF, to evaluate the degree of risk presented by the jurisdiction in which the Respondent and/or its parent are based.

- ***The Respondent's ownership and management structures.*** *The location of owners, their corporate legal form and/or a lack of transparency of the ultimate beneficial ownership are indicative of the risk the Respondent presents. Account should be taken of whether the Respondent is publicly or privately owned; if publicly held, whether its shares are traded on a recognised market or exchange in a jurisdiction with a satisfactory regulatory regime, or, if privately owned, the identity of any beneficial owners and controllers. Similarly, the location and experience of management may indicate additional concerns, as would unduly frequent management turnover. The involvement of PEPs in the management or ownership of certain Respondents may also increase the risk.*

- ***The Respondent's business and customer base.*** *The type of business the Respondent engages in, as well as the type of markets it serves, is indicative of the risk the Respondent presents. Involvement in certain business segments that are recognised internationally as particularly vulnerable to money laundering, corruption or terrorist financing, may present additional concern. Consequently, a Respondent that derives a substantial part of its business income from higher risk customers may present greater risk. Higher risk customers are those customers that may be involved in activities, or are connected to jurisdictions, that are identified by credible sources as activities or countries being especially susceptible of money laundering/terrorist financing or corruption. […]*

Customer due diligence

34. Paragraph 16.15 states:

The Correspondent in assessing the level of due diligence to be carried out in respect of a particular Respondent, (in addition to the issues raised in paragraph 16.9) must consider:

- ***Regulatory status and history.*** *The primary regulatory body responsible for overseeing or supervising the Respondent and the quality of that supervision. If circumstances warrant, a Correspondent should also consider publicly available materials to ascertain whether the Respondent has been the subject of any criminal case or adverse regulatory action in the recent past.*

- ***AML/CTF controls.*** *A Correspondent should establish whether the Respondent is itself regulated for money laundering/terrorist financing prevention and, if so, whether the Respondent is required to verify the identity of its customers and apply other AML/CTF controls to FATF standards/equivalent to those laid down in the money laundering directive. Where this is not the case, additional due diligence should be undertaken to ascertain and assess the effectiveness of the Respondent's internal policy*

on money laundering/terrorist financing prevention and its know your customer and activity monitoring controls and procedures. Where undertaking due diligence on a branch, subsidiary or affiliate, consideration may be given to the parent having robust group-wide controls, and whether the parent is regulated for money laundering/terrorist financing to FATF standards/equivalent to those laid down in the money laundering directive. If not, the extent to which the parent's controls meet FATF standards/equivalent to those laid down in the money laundering directive and whether these are communicated and enforced 'effectively' throughout its network of international offices, should be ascertained. […]

Enhanced due diligence

35. Paragraph 16.17 states:

Correspondents are required by Regulation 14(3) of the ML Regulations to subject Respondents from non-EEA States to enhanced customer due diligence, but should consider doing so whenever the Respondent has been considered to present a greater money laundering/terrorist financing risk. The enhanced due diligence process should involve further consideration of the following elements designed to ensure that the Correspondent has secured a greater level of understanding:

- ***Respondent's ownership and management.*** *For all beneficial owners and controllers, the sources of wealth and background, including their reputation in the market place, as well as recent material ownership changes (e.g. in the last three years). Similarly, a more detailed understanding of the experience of each member of executive management as well as recent material changes in the executive management structure (e.g., within the last three years).*

- ***Respondent's business.*** *Gather sufficient information about the Respondent to understand fully the nature of its business. In addition, determine from publicly available information the reputation of the Respondent and the quality of its supervision.*

- ***PEP involvement.*** *If a PEP (see Part I, paragraphs 5.5.18-5.5.30) appears to have a material interest or management role in a Respondent then the Correspondent should ensure it has an understanding of that person's role in the Respondent.*

  Respondent's anti-money laundering/terrorist financing controls. *An assessment of the quality of the Respondent's AML/CTF and customer identification controls, including whether these controls meet internationally recognised standards. The extent to which a Correspondent should enquire will depend upon the perceived risks. Additionally, the Correspondent may wish to speak with representatives of the Respondent to obtain comfort that the Respondent's senior management recognise the importance of anti-money laundering/terrorist financing controls. […]*

36. Paragraph 16.21 states:

In addition to monitoring account/transaction activity, a Correspondent should monitor a Respondent for changes in its nature and status. As such, information about the Respondent collected during the customer acceptance and due diligence processes must be:

- *Reviewed and updated on a periodic basis. (Periodic review of customers will occur on a risk-assessed basis), or*

- *Reviewed on an ad hoc basis as a result of changes to the customers information identified during normal business practices, or*

- *Reviewed when external factors result in a material change in the risk profile of the customer.*

37. Paragraph 16.22 states:

Where such changes are identified, the Respondent should be subject to a revised risk assessment, and a revision of their risk categorisation, as appropriate. Where, as a result of the review, the risk categorisation is altered (either up or down) a firm should ensure that the due diligence standards for the Respondent's new risk categorisation are complied with, by updating the due diligence already held. In addition, the level of monitoring undertaken should be adjusted to that appropriate for the new risk category.

38. Paragraph 16.24 states:

The firm will need to have a means of assessing that its risk mitigation procedures and controls are working effectively. In particular the firm will need to consider:

- *Reviewing ways in which different services may be used for ML/TF purposes, and how these ways may change, supported by typologies/law enforcement feedback, etc.;*

- *Adequacy of staff training and awareness;*

- *Capturing appropriate management information;*

- *Upward reporting and accountability; and*

- *Effectiveness of liaison with regulatory and law enforcement agencies.*

ANNEX B – PENALTY ANALYSIS

1. BACKGROUND

1.1. The application of the Authority's penalty policy is set out below in relation to SCB's breaches of the ML Regulations relating to:

a. The UK Wholesale Bank's Correspondent Banking business (Section 2);

b. SCB's UAE branches to the extent it relates to the Consumer Bank (Section 3); and

c. SCB's UAE branches to the extent it relates to the Wholesale Bank (Section 4).

1.2. References to DEPP in this Notice are to the version in force during the Relevant Period.

2. FAILINGS RELATING TO THE UK WHOLESALE BANK'S CORRESPONDENT BANKING BUSINESS

Step 1: disgorgement

2.1. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

2.2. The Authority has not identified any financial benefit that SCB derived directly from its breaches.

2.3. Step 1 is therefore £0.

Step 2: the seriousness of the breach

2.4. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

2.5. The Authority considers that the revenue generated by SCB is indicative of the harm or potential harm caused by its breaches. The Authority has therefore determined a figure based on a percentage of SCB's relevant revenue. SCB's relevant revenue is the revenue derived from the UK Wholesale Bank during the period of the breach. The period of SCB's breaches in relation to the UK Wholesale Bank's Correspondent Banking business was from 11 November 2010 to 22 July 2013 inclusive. The Authority considers SCB's relevant revenue for its failings relating to the UK Wholesale Bank's Correspondent Banking business for this period to be £137,150,784.

2.6. In deciding on the percentage of the relevant revenue that forms the basis of the Step 2 figure, the Authority considers the seriousness of the breaches and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breaches; the more serious the breaches, the higher the level. For penalties imposed on firms there are the following five levels:

- Level 1 – 0%
- Level 2 – 5%
- Level 3 – 10%
- Level 4 – 15%
- Level 5 – 20%

2.7. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breaches. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

a. *"the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business"*; and

b. *"the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur."*

2.8. DEPP 6.5A.2G(12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

a. *"little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly"; and*

b. *"the breach was committed negligently or inadvertently"*.

2.9. Taking all of these factors into account, the Authority considers the seriousness of the failings to be level 4 and so the Step 2 figure is 15% of £137,150,784.

2.10. Step 2 is therefore £20,572,618.

Step 3: mitigating and aggravating factors

2.11. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

2.12. The Authority considers that the following factors aggravate the breaches:

a. the Authority visited SCB in November 2010 as part of a thematic review of SCB's AML processes. A feedback letter sent to SCB in November 2010 following this visit highlighted weaknesses in SCB's AML systems and controls in relation to Correspondent Banking;

b. the Authority has published guidance on the steps firms can take to reduce their financial crime risk and provided examples of good and bad practice since 2011. Since 1990, the JMLSG has published detailed written guidance on AML controls. During the Relevant Period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving practice within the financial services industry. Before, or during, the CB Relevant Period, the Authority published the following guidance relating to AML controls, which set out good practice examples to assist firms in interpreting the ML Regulations:

i. in March 2008, the Authority published a report titled "Review of firms' implementation of a risk-based approach to anti-money laundering". In

respect of Correspondent Banking relationships, the report notes that there is a need for the Correspondent to review the Respondent's ownership and management, any PEP involvement and the Respondent's AML controls;

ii. in June 2011, the Authority published a report titled "Banks' management of high money-laundering risk situations: How banks deal with high-risk customers (including politically exposed persons), correspondent banking relationships and wire transfers". The report notes that if banks fail to implement appropriate controls when accepting Correspondent Banking relationships, this can give banks with inadequate AML systems and controls access to the international banking system; and

iii. in December 2011, the Authority published "Financial Crime: A Guide for Firms". The guide highlights the need to conduct adequate customer due diligence checks, perform ongoing monitoring and carry out enhanced due diligence measures and enhanced ongoing monitoring when handling higher risk situations, including PEPs and Correspondent Banking relationships.

SCB accordingly had access to considerable guidance on how to comply with regulatory requirements and should have been aware of the importance of implementing and maintaining robust AML systems and controls; and

c. the Authority has published a number of Final Notices against firms for AML weaknesses both before and during the Relevant Period, including Alpari (UK) Limited on 5 May 2010, Coutts & Company on 23 March 2012, Habib Bank AG Zurich on 4 May 2012, Turkish Bank (UK) Limited on 26 July 2012 and EFG Private Bank Ltd on 28 March 2013. These actions stressed to the industry the Authority's view of firms with AML deficiencies especially in relation to higher risk customers. SCB was accordingly aware of the importance of implementing and maintaining robust AML systems and controls, and its importance to the Authority.

2.13. Given the points in paragraph 2.12, SCB was aware, or should have been aware, of the importance of putting in place and maintaining effective procedures to detect and prevent money laundering.

2.14. The Authority considers that the following factors mitigate the breaches:

a. as referred to in paragraph 4.123c, SCB has significantly increased the resource dedicated to managing financial crime risk. The number of AML professionals employed by SCB has approximately quadrupled since the end of 2012. SCB has also made key strategic appointments in senior roles, including appointing a new Global Head of Financial Crime Compliance;

b. SCB has set up a Financial Crime Compliance Correspondent Banking Academy as referred to in paragraph 4.123h;

c. since late 2013 SCB has been working on a global financial crime risk mitigation programme to improve its financial crime risk management framework, covering AML, sanctions, as well as anti-bribery and corruption-related systems and controls. As part of this programme, SCB has been conducting a significant CDD remediation project including in relation to Correspondent Banking; and

d. the degree of SCB's co-operation during the Authority's investigation is a mitigating factor. This included ensuring that senior management was engaged from the outset, conducting extensive and wide-ranging internal investigations and reporting the conclusions of those investigations to the Authority in a fully transparent manner.

2.15. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.

2.16. Step 3 is therefore £22,629,879.

Step 4: adjustment for deterrence

2.17. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

2.18. The Authority considers that the Step 3 figure of £22,629,879 represents a sufficient deterrent to SCB and others, and so has not increased the penalty at Step 4.

2.19. Step 4 is therefore £22,629,879.

Step 5: settlement discount

2.20. The Authority and SCB reached agreement at stage 1 in relation to all relevant facts and all issues as to whether those facts constitute breaches, and so a 30% discount applies to the Step 4 figure.

2.21. Step 5 is therefore £15,840,915.

3. CONSUMER BANK FAILINGS RELATING TO SCB'S UAE BRANCHES

Step 1: disgorgement

3.1. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

3.2. The Authority has not identified any financial benefit that SCB derived directly from its breaches.

3.3. Step 1 is therefore £0.

Step 2: the seriousness of the breach

3.4. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

3.5. The Authority considers that the revenue generated by SCB's Consumer Bank is indicative of the harm or potential harm caused by its breaches. The Authority has therefore determined a figure based on a percentage of the Consumer Bank's relevant revenue. The relevant revenue is the revenue derived by the Consumer

Bank from SCB's UAE branches during the period of the breach. The period of the Consumer Bank's breaches in relation to SCB's UAE branches was from 24 November 2009 to 31 December 2014 inclusive. The Authority considers SCB's Consumer Bank's relevant revenue for its failings relating to its UAE branches for this period to be £1,177,834,325.

3.6. In deciding on the percentage of the relevant revenue that forms the basis of the Step 2 figure, the Authority considers the seriousness of the breaches and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breaches; the more serious the breaches, the higher the level. For penalties imposed on firms there are the following five levels:

- Level 1 – 0%
- Level 2 – 5%
- Level 3 – 10%
- Level 4 – 15%
- Level 5 – 20%

3.7. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breaches. DEPP 6.5A.2G (11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

a. *"the breach revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business"*; and

b. *"the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur"*.

3.8. Taking these factors into account, the Authority considers the seriousness of the failings to be level 4 and so the Step 2 figure is 15% of £1,177,834,325.

3.9. Step 2 is therefore £176,675,149.

3.10. Pursuant to DEPP 6.5.3(3)G, the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breaches concerned. Notwithstanding the serious and long-running nature of the breaches, the Authority considers that the level of penalty would nonetheless be disproportionate if it were not reduced and should be adjusted.

3.11. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £70,670,059.

Step 3: mitigating and aggravating factors

3.12. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

3.13. The Authority considers that the following factors aggravate these breaches:

a. the Authority visited SCB in October 2012 and April 2013 as part of a thematic review of the firm's CTF and sanctions controls. A feedback letter sent to SCB

in July 2013 highlighted a number of weaknesses in sanctions controls. SCB was accordingly aware of the importance of implementing and maintaining robust AML systems and controls;

b. actions taken by US authorities against SCB during the Relevant Period highlighted: i. issues with SCB's financial crime internal controls generally and in the UAE; and ii. financial crime risks associated with conducting business with Iranian nationals in the UAE;

c. the Authority has published guidance on the steps firms can take to reduce their financial crime risk and provided examples of good and bad practice since 2011. Since 1990, the JMLSG has published detailed written guidance on AML controls. During the Relevant Period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving practice within the financial services industry. Before, or during, the Relevant Period, the Authority published the guidance relating to AML controls noted in paragraph 2.12b of Annex B. SCB accordingly had access to considerable guidance on how to comply with regulatory requirements and should have been aware of the importance of implementing and maintaining robust AML systems and controls; and

d. the Authority has published a number of Final Notices against firms for AML weaknesses both before and during the Relevant Period, including Alpari (UK) Limited on 5 May 2010, Coutts & Company on 23 March 2012, Habib Bank AG Zurich on 4 May 2012, Turkish Bank (UK) Limited on 26 July 2012, EFG Private Bank Ltd on 28 March 2013, Guaranty Trust Bank (UK) Ltd on 8 August 2013 and Standard Bank Plc on 22 January 2014. These actions stressed to the industry the Authority's view of firms with AML deficiencies especially in relation to higher risk customers. SCB was accordingly aware of the importance of implementing and maintaining robust AML systems and controls, and its importance to the Authority.

3.14. Given the points in paragraph 3.13, SCB was aware, or should have been aware, of the importance of putting in place and maintaining effective procedures to detect and prevent money laundering.

3.15. The Authority considers that the following factors mitigate the breaches:

a. as referred to in paragraph 4.123c, SCB has significantly increased the resource dedicated to managing financial crime risk. The number of AML professionals employed by SCB has approximately quadrupled since the end of 2012. SCB has also made key strategic appointments in senior roles, including appointing a new Global Head of Financial Crime Compliance;

b. since late 2013 SCB has been working on a global financial crime risk mitigation programme to improve its financial crime risk management framework, covering AML, sanctions, as well as anti-bribery and corruption-related systems and controls. As part of this programme, SCB has been conducting a significant CDD remediation project including in relation to its UAE branches;

c. in the United States, SCB also formed an association of financial institutions to improve how banks identify and report suspected financial crime, working with law enforcement and other government agencies; and

d. the degree of SCB's co-operation during the Authority's investigation is a mitigating factor. This included ensuring that senior management was engaged from the outset, conducting extensive and wide-ranging internal investigations and reporting the conclusions of those investigations to the Authority in a fully transparent manner.

3.16. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.

3.17. Step 3 is therefore £77,737,065.

Step 4: adjustment for deterrence

3.18. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

3.19. The Authority considers that the Step 3 figure of £77,737,065 represents a sufficient deterrent to SCB and others, and so has not increased the penalty at Step 4.

3.20. Step 4 is therefore £77,737,065.

Step 5: settlement discount

3.21. The Authority and SCB reached agreement at stage 1 in relation to all relevant facts and all issues as to whether those facts constitute breaches and so a 30% discount applies to the Step 4 figure.

3.22. Step 5 is therefore £54,415,946.

4. WHOLESALE BANK FAILINGS RELATING TO SCB'S UAE BRANCHES

Step 1: disgorgement

4.1. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

4.2. The Authority has not identified any financial benefit that SCB derived directly from its breaches.

4.3. Step 1 is therefore £0.

Step 2: the seriousness of the breach

4.4. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

4.5. The Authority considers that the revenue generated by SCB's Wholesale Bank is indicative of the harm or potential harm caused by its breaches. The Authority has therefore determined a figure based on a percentage of the Wholesale Bank's relevant revenue. The relevant revenue is the revenue derived by the Wholesale

Bank from SCB's UAE branches during the period of the breach. The period of the Wholesale Bank's breaches in relation to SCB's UAE branches was from 24 November 2009 to 31 December 2014 inclusive. The Authority considers SCB's Wholesale Bank's relevant revenue for its failings relating to its UAE branches for this period to be £2,071,843,541.

4.6. In deciding on the percentage of the relevant revenue that forms the basis of the Step 2 figure, the Authority considers the seriousness of the breaches and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breaches; the more serious the breaches, the higher the level. For penalties imposed on firms there are the following five levels:

- Level 1 – 0%
- Level 2 – 5%
- Level 3 – 10%
- Level 4 – 15%
- Level 5 – 20%

4.7. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breaches. DEPP 6.5A.2G (11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factor to be relevant:

a. *"the breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur".*

4.8. DEPP 6.5A.2G (12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

a. *"there is no evidence that the breach indicates a widespread problem or weakness at the firm"*; and

b. *"the breach was committed negligently or inadvertently"*.

4.9. Taking all of these factors into account, the Authority considers the seriousness of the failings to be level 3 and so the Step 2 figure is 10% of £2,071,843,541.

4.10. Step 2 is therefore £207,184,354.

4.11. Pursuant to DEPP 6.5.3(3)G, the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breaches concerned. Notwithstanding the serious and long-running nature of the breaches, the Authority considers that the level of penalty would nonetheless be disproportionate if it were not reduced and should be adjusted.

4.12. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £41,436,871.

Step 3: mitigating and aggravating factors

4.13. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

4.14. The Authority considers that the following factors aggravate these breaches:

a. the Authority visited SCB in October 2012 and April 2013 as part of a thematic review of the firm's CTF and sanctions controls. A feedback letter sent to SCB in July 2013 highlighted a number of weaknesses in sanctions controls. SCB was accordingly aware of the importance of implementing and maintaining robust AML systems and controls;

b. actions taken by US authorities against SCB during the Relevant Period highlighted: i. issues with SCB's financial crime internal controls generally and in the UAE; and ii. financial crime risks associated with conducting business with Iranian nationals in the UAE;

c. the Authority has published guidance on the steps firms can take to reduce their financial crime risk and provided examples of good and bad practice since 2011. Since 1990, the JMLSG has published detailed written guidance on AML controls. During the Relevant Period, the JMLSG provided guidance on compliance with the legal requirements of the ML Regulations, regulatory requirements in the Handbook and evolving practice within the financial services industry. Before, or during, the Relevant Period, the Authority published the guidance relating to AML controls noted in paragraph 2.12b of Annex B. SCB accordingly had access to considerable guidance on how to comply with regulatory requirements and should have been aware of the importance of implementing and maintaining robust AML systems and controls; and

d. the Authority has published a number of Final Notices against firms for AML weaknesses both before and during the Relevant Period, including Alpari (UK) Limited on 5 May 2010, Coutts & Company on 23 March 2012, Habib Bank AG Zurich on 4 May 2012, Turkish Bank (UK) Limited on 26 July 2012, EFG Private Bank Ltd on 28 March 2013, Guaranty Trust Bank (UK) Ltd on 8 August 2013 and Standard Bank Plc on 22 January 2014. These actions stressed to the industry the Authority's view of firms with AML deficiencies especially in relation to higher risk customers. SCB was accordingly aware of the importance of implementing and maintaining robust AML systems and controls, and its importance to the Authority.

4.15. Given the points in paragraph 4.14, SCB was aware, or should have been aware, of the importance of putting in place and maintaining effective procedures to detect and prevent money laundering.

4.16. The Authority considers that the following factors mitigate the breaches:

a. as referred to in paragraph 4.123c, SCB has significantly increased the resource dedicated to managing financial crime risk. The number of AML professionals employed by SCB has approximately quadrupled since the end of 2012. SCB has also made key strategic appointments in senior roles, including appointing a new Global Head of Financial Crime Compliance;

b. since late 2013 SCB has been working on a global financial crime risk mitigation programme to improve its financial crime risk management framework, covering AML, sanctions, as well as anti-bribery and corruption-related systems and controls. As part of this programme, SCB has been conducting a significant CDD remediation project including in relation to its UAE branches;

c. in the United States, SCB also formed an association of financial institutions to improve how banks identify and report suspected financial crime, working with law enforcement and other government agencies; and

d. the degree of SCB's co-operation during the Authority's investigation is a mitigating factor. This included ensuring that senior management was engaged from the outset, conducting extensive and wide-ranging internal investigations and reporting the conclusions of those investigations to the Authority in a fully transparent manner.

4.17. Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.

4.18. Step 3 is therefore £45,580,558.

Step 4: adjustment for deterrence

4.19. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm that committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

4.20. The Authority considers that the Step 3 figure of £45,580,558 represents a sufficient deterrent to SCB and others, and so has not increased the penalty at Step 4.

4.21. Step 4 is therefore £45,580,558.

Step 5: settlement discount

4.22. The Authority and SCB reached agreement at stage 1 in relation to all relevant facts and all issues as to whether those facts constitute breaches and so a 30% discount applies to the Step 4 figure.

4.23. Step 5 is therefore £31,906,391.

5. TOTAL PENALTY

5.1. The Authority has therefore decided to impose a total financial penalty (rounded down to the nearest £100) of £102,163,200 (£145,947,500 before 30% (stage 1) discount) on SCB for breaching Regulations 14(3), 15(1) and 20(1) of the ML Regulations. Of the penalty, £86,322,300 (£123,317,600 before 30% (stage 1) discount) relates to failings in SCB's oversight of its UAE branches, and £15,840,900 (£22,629,800 before 30% (stage 1) discount) relates to Correspondent Banking failings.

ANNEX C – REPRESENTATIONS

1. SCB's representations (in italics), and the Authority's conclusions in respect of them, are set out below:

Wholesale Bank UAE branches - relevant revenue

2. *As a result of the decision to include the entirety of the Wholesale Bank's UAE Branches' ('UAE WB') revenue at Step 2 of the UAE WB penalty calculation, UAE WB revenue comprises nearly two thirds of the aggregate relevant revenue figure used to arrive at the total penalty. The nature and, in the context, small scale of the UAE WB breaches does not justify the inclusion of the entirety of UAE WB revenue, nor the resulting impact of this revenue amount on the penalty as a whole. The decision to include the entirety of WB UAE revenue is excessive and unduly severe. The breaches identified in the Notice do not relate to the entirety of the UAE WB business.*

3. *The breaches found in relation to UAE WB arise primarily from three sources: (a) the review of GIC files; (b) S2B access from Iran by UAE WB customers; and (c) faxed payment instructions sent from Iran. The small number of these breaches are not indicative of a larger problem in the UAE WB segment.*

4. *For these reasons, the entirety of the UAE WB revenue cannot be an appropriate starting point for Step 2. The Notice should adopt a considerably smaller percentage of revenue as relevant to the breaches. Using the entirety of UAE WB's revenue as the relevant revenue produces a figure that greatly overstates the revenue which was at risk of being impacted by the agreed breaches. This can be remedied by reducing the relevant revenue figure. For example, the Authority could take as the relevant revenue the value of the S2B and faxed payment instructions transactions identified (i.e. $16,867,022.33) or 0.6% of UAE WB revenue to reflect the GIC files found to have deficiencies (i.e. £12,431,061.25).*

5. *Alternatively, if the Authority decides to retain the entire UAE WB revenue as relevant revenue, the appropriate consequence would be (after applying the appropriate seriousness level) to increase significantly the proportionality discount for the UAE WB penalty over what would otherwise be appropriate, on the basis that the overstated harm or potential harm means that the revenue figure is not proportionate to the breaches.*

6. The Authority has concluded that it is appropriate to include the entirety of UAE WB revenue at Step 2 of the UAE WB penalty calculation – this is the "relevant revenue". The definition of "relevant revenue" in DEPP 6.5A.2G(2) provides that it "will be the revenue derived by the firm during the period of the breach from the products or business areas to which the breach relates". This definition does not restrict the revenue to that derived solely from the relevant activity affected by the breach, as it encompasses all revenue derived "from the products or business areas" to which the breach relates. Accordingly, as long as the revenue received by the firm derives from the relevant product or business area it should be included.

7. Based on the facts and breaches accepted by SCB in sections 4 and 5 of this Notice it is clear that the UAE WB breaches were not limited to the instances SCB identifies above. Further, SCB accepts that the entirety of the Consumer Bank UAE branches' ('UAE CB') revenue is an appropriate starting point in calculating the UAE CB penalty, and the Notice draws no material distinction between the breaches of the UAE CB and UAE WB (which are not separate legal entities). The Authority therefore considers it appropriate for the entirety of the UAE WB revenue to be the starting point for the UAE WB penalty calculation.

8. The Authority recognises, however, that although the breaches set out in the Notice affected both the UAE CB and UAE WB, the impact on the UAE WB of the breaches was less than on the UAE CB. In calculating the appropriate penalties the Authority has therefore made adjustments to account for this. The UAE WB seriousness level at Step 3 of the calculation has been set at 3, as opposed to the level 4 seriousness for the UAE CB. In addition, a larger proportionality discount has been applied in the penalty calculation for the UAE WB than for the UAE CB.

9. The Authority deals with SCB's arguments in relation to proportionality in the relevant section below.

UK Wholesale Bank correspondent banking – seriousness level

10. *The nature and scale of the breaches relating to the UK Wholesale Bank correspondent banking business ('UK WB') provide no reasonable basis to apply Level 4 seriousness to such findings. The appropriate outcome would be to apply Level 3 seriousness.*

11. *At DEPP 6.5A.2G(12), the Authority sets out factors likely to be considered Level 3 factors. They include four factors that are present here:*

    (a) Little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly;
    (b) No or little loss or risk of loss to consumers, investors or other market users individually and in general;
    (c) No, or limited, actual or potential effect on the orderliness of, or confidence in, markets as a result of the breach; and
    (d) Whether the breach was committed negligently or inadvertently.

12. *Only two factors exist that could be said to be Level 4 or 5 factors. Whilst SCB recognises that the seriousness level is not determined merely by counting the number of relevant factors, it is highly relevant to the exercise of determining the seriousness level that four of the Level 3 factors are present. Further, a number of the Authority's Level 4 factors are plainly not present in relation to the UK WB business, namely:*

    (a) the breach caused a significant loss or risk of loss to individual consumers, investors or other market users;
    (b) the firm failed to conduct its business with integrity; or
    (c) the breach was committed deliberately or recklessly.

13. *The Bank acknowledges and accepts the finding that there were serious and sustained shortcomings in relation to customer due diligence and ongoing monitoring. But this fact alone should not elevate the UK WB penalty to Level 4 seriousness (and has not done so for the UAE WB business), especially when faced with the wider analysis of applicable factors.*

14. *When considered in this context, there is simply no justification for the breaches in relation to the UK WB to be treated as anything other than Level 3 seriousness.*

15. As set out in the facts and matters in this Notice, and agreed by SCB, in relation to UK WB:

    (a) the business is a higher risk segment;
    (b) there were serious and systematic Due Diligence shortcomings (including failings in 100% of the 67 Correspondent Banking files reviewed by the

Authority) which were particularly egregious given the high volume and value of SCB's Correspondent Banking transactions during the CB Relevant Period and the high risk of the jurisdictions in which it operated;

(c) it was particularly serious that SCB had no Due Diligence records for a small number of the UK WB's non-EEA Correspondent Banking relationships as it exposed SCB to increased levels of financial crime risk; and

(d) there were widespread failures in SCB's reviews of Due Diligence conducted as part of its ongoing monitoring of AML risks from customer accounts for the UK Wholesale Bank's Correspondent Banking files.

16. The serious and systemic weaknesses in the CDD policies and procedures across all of SCB's global offices and the accompanying significant risk of financial crime are sufficiently serious to indicate that this aspect of the case should be of level 4 seriousness. The Authority accepts that the points set out at paragraph 11(a) and (d) above are relevant, and has included these in the relevant penalty section in Annex B above. The Authority does not accept that the factors set out at paragraph 11(b) and (c) above are relevant. In any event, even if all four factors were present, the Authority does not consider them sufficient to outweigh the global nature of the failings or the risk of financial crime.

17. As set out in this Notice the Authority considers that the UAE WB business breaches, based on the factors relevant to that specific misconduct, are of seriousness level 3. The Authority does not consider this to be inconsistent, given the different factors relevant to that misconduct.

Proportionality

18. *The Step 2 figure is disproportionately high for the breaches concerned. In this context, it is instructive to have regard to the approach taken to proportionality in other enforcement actions by the Authority. In particular, SCB draws a comparison to the Final Notice given to Deutsche Bank AG ('Deutsche Bank') dated 30 January 2017 as being a highly relevant precedent. One can and must compare in each case the seriousness of the respective breaches, and the potential impact of the breaches (by the proxy of the relevant revenue). One then looks at the consistency of the reduction said to be appropriate to render the penalty proportionate. That comparison exercise is compelling between Deutsche Bank's case and this case, because both cases involve serious and sustained shortcomings in AML/financial crime systems and controls.*

19. *In Deutsche Bank's case, the breaches were all found to be of seriousness Level 4. That compares with the findings of seriousness in this case at Level 3 (UAE WB) or Level 4 (UK WB and UAE CB). As noted above, SCB contends that the UK WB should be treated as Level 3, but in any event the overall level of seriousness is lower here than in Deutsche Bank's case.*

20. *Relevant revenue is intended to reflect the harm or potential harm of a breach (see DEPP 6.5A.2G(2)): it is the revenue which is at least potentially implicated by the breach(es). Where a breach results in widespread harm or potential harm (and therefore there is a large relevant revenue) then one would expect the Step 2 figure to be large. What Deutsche Bank's high starting revenue shows is that the harm or potential harm flowing from the breach was exceptionally large: over three times higher than here. The high starting revenue does not provide grounds for a larger proportionate reduction than in SCB's case. Where (as here) the relevant revenue is not a good proxy for the harm or potential harm caused by a breach then a very substantial reduction in percentage terms is needed to provide a proportionate penalty. SCB has a strong argument not found in Deutsche Bank's case that the*

relevant revenue is a particularly poor proxy for potential harm here, because of the extremely low levels of harm in fact found or realistically apprehended.

21. *In comparing this case with Deutsche Bank's it is therefore notable that the harm or potential harm (as calculated through the relevant revenue) caused by the Bank's breaches is much smaller, and the level of seriousness of SCB's breaches has been assessed to be the same or lower. In further contrast with Deutsche Bank, SCB has not made any identifiable financial gain; and there has been no history of regulatory enforcement in the UK.*

22. *The Deutsche Bank Notice overall gives a percentage reduction of over 88% on the pre-reduction Step 2 figure. That percentage discount greatly exceeds the proportionality discount in this case. In considering proportionality (and the overall penalty figure) the Authority can consider the three penalty calculations separately, but should also step back and consider the total figure.*

23. *For the reasons given above, the approach at Step 2 has generated a figure that is disproportionate to SCB's breaches. In the circumstances, the total Step 2 figure should be lower than the £171,065,499 proposed by the Authority and should not exceed £46,509,694 - the figure that results from applying the same proportionality reduction as was applied in the Deutsche Bank Final Notice to the relevant revenues identified in this Notice - and should in fact be significantly lower. The overall penalty should not be the £155,669,600 proposed by the Authority and should instead be significantly less than £35,812,464 (including a 10% overall uplift for aggravating/mitigating factors and 30% settlement discount).*

24. DEPP 6.5.3G(3) states that "The [Authority] recognises that a penalty must be proportionate to the breach. The [Authority] may decrease the level of the penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breach concerned." This Notice sets out, in detail, SCB's very serious misconduct, which SCB has accepted. The Authority considers that the Step 2 figure for the UK WB breaches is proportionate. However, the Authority accepts that in this case the figures produced at Step 2, before any proportionality discount is applied, are disproportionately high for the relevant breaches, in respect of both the UAE CB and UAE WB.

25. The proportionality assessment can be seen as a "sense-check", whereby the Authority stands back and considers whether the Step 2 penalty figure is a proportionate sanction in relation to the misconduct that occurred. Other cases can be useful as comparators, and the Authority accepts that there are similarities between this case and the Deutsche Bank case.

26. In all the circumstances, taking into account the nature of the breaches, the Authority considers that reducing the UAE WB figure by 80%, and the UAE CB figure by 60%, produces proportionate figures at Step 2.

27. As set out in Annex B to this Notice, the Authority has considered the three penalty calculations separately. However, when considered overall the Authority also considers that the total penalty is proportionate and appropriate.

Mitigating and aggravating factors

28. *The mitigating and aggravating factors should result in a Step 3 adjustment significantly less severe than the 10% increase applied to Deutsche Bank, particularly given the long history of enforcement action taken by the Authority against Deutsche Bank, as set out in Deutsche Bank's Final Notice.*

29. As set out in the penalty calculations in Annex B of this Notice, taking into account the mitigating and aggravating factors relevant in this case, the Authority considers the appropriate adjustment at Step 3 is an uplift of 10%. Although all cases, and mitigation/aggravation adjustments, are assessed on their own specific facts, the Authority considers that its approach to assessing mitigating and aggravating factors in this case is consistent with the approach in the Deutsche Bank case, taking into account the factors set out in this Notice and those in the Deutsche Bank Final Notice.